Cultivating Cybersecurity Defence Expertise with Mindful Readiness and Skills

WP2 – Cybersecurity Skills Needs Analysis and Specification

D2.1 Cybersecurity Training Initiatives Map, Skills Gap and Specifications

PARTNERS

NATIONAL CYBERSECURITY AUTHORITY (NCSA)

COMPUTER TECHNOLOGY INSTITUTE AND PRESS “DIOPHANTUS” (CTI)

STICHTING THE HAGUE SECURITY DELTA (HSD)

STICHTING CENTRUM VOOR VEILIGHEID EN DIGITALISERING (CVD)

SVEUCILISTE ALGEBRA (AU)

DIGITAL SECURITY AUTHORITY (DSA)

EUROPEAN UNIVERSITY - CYPRUS LTD (EUC)

Digital Europe Programme (DIGITAL)		
Project title	Cultivating Cybersecurity Defence Expertise with Mindful Readiness and Skills	
Project Acronym	CADMUS	
Grant Agreement number	101190006	
Call Topic/Type of action	DIGITAL-2023-SKILLS-05-CYBERACADEMY/DIGITAL-SIMPLE	
Project start date	1 December 2024	
Project duration	36	
Deliverable number	D2.1	
Deliverable Name	Cybersecurity Training Initiatives Map, Skills Gap and Specifications	
Deliverable doc. version	v8	
Deliverable type	☒ R - Document, report	☐ DEM - Demonstrator, pilot, prototype
Dissemination level	☒ PU – Public	☐ SEN – Sensitive
Lead Beneficiary	HSD	
Contributing Partners	NCSA, CTI, CVD, AU, DSA, EUC	
Author(s)	Mark Ruijsendaal, Max Kroes, Mira van Benthem (HSD), Carine van Vliet, Stephan Corporaal (CVD), Zlatan Morić (AU), Yiorgos Stergiopoulos, Dimitris Gritzalis (CTI), Socratis Socratous, Polis Peratikos (DSA), Yianna Danidou (EUC), Ioannis Alexakis (NCSA)	
Contributor(s)	Alexandra Hattink, Yanic Hoch, Simone Hefting (HSD), Sjoerd Peters, Nikki Wamelink (CVD), Martina Golubić Goronja, Tomislav Dominkovic (AU), Christos Zaroliagis (CTI), Dora Nousia (CTI)	
Internal reviewer(s)	Emmanouil Patsourakis (NCSA) and Saskia Noordewier (HSD)	
Due submission date	31/08/2025	
Actual submission date	31/08/2025	

HISTORY OF CHANGES

No	Date	Issued by	Ver	Short Description of Changes.
01	07/03/2025	Mark Ruijsendaal	v1	First setup of the document structure and expected inputs.
02	13/06/2025	Max Kroes, Alexandra Hattink	v2	Extending the document structure to provide guidance for expected inputs.
03	08/07/2025	Mark Ruijsendaal, Mira van Benthem	v3	Cleaned up intermediate version for informal check by PO HADEA.
04	15/08/2025	Max Kroes	v4	Revising data inputs, analyses, tables. Restructuring document to enhance readability.
05	16/08/2025	Mark Ruijsendaal, Max Kroes, Mira van Benthem, Stephan Corporaal	v5	Renewed GAP-analysis, changes to all chapters, updated table chapter 8.
06	17/08/2025	Mark Ruijsendaal	v6	Remarks removed, graphs added, inputs for chapter 7. Concept version for internal review.
07	18/08/2025	Dimitris Gritzalis	v7	Changed inputs for chapter 7. Concept version for internal review.
08	28/08/2025	Mark Ruijsendaal	v8	Changes throughout the document based on internal review by Emmanouil Patsourakis and Saskia Noordewier.

TABLE OF CONTENTS

DEFINITIONS, ABBREVIATIONS & ACRONYMS

AI	**A**rtificial **I**ntelligence is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.
APIs	**A**pplication **P**rogramming **I**nterfaces is a set of rules or protocols that enables software applications to communicate with each other.
ARIA	**A**ccessible **R**ich **I**nternet **A**pplications is a set of roles and attributes that define ways to make web content and web applications (especially those developed with JavaScript) more accessible to people with disabilities.
Bologna process	Process of harmonizing various systems of European higher education.
CADMUS	**C**ultivating **C**ybersecurity **D**efence **E**xpertise with **M**indful **R**eadiness and **S**kills.
CEH	**C**ertified **E**thical **H**acker is a certification provided by EC-Council and a well-known ethical hacking course in the cybersecurity industry.
CEN	European Committee for Standardisation (CEN) is an association of national standardisation bodies from 33 European countries that develops and promotes voluntary technical standards for a wide range of products, materials, and services across Europe.
CERTs	**C**ybersecurity **E**mergency **R**esponse **T**eams are the first responders in the event of a cyberattack.
CI/CD	**C**ontinuous **I**ntegration/**C**ontinuous **D**elivery aims to streamline and accelerate the software development lifecycle.
CISA	**C**ybersecurity and **I**nfrastructure **S**ecurity **A**gency is USA's Cyber Defense Agency, a component of the United States Department of Homeland Security.
CISM	**C**ertified **I**nformation **S**ecurity **M**anager is a certification provided by ISACA and a well-known course in the cybersecurity industry.
CISO	**C**hief **I**nformation **S**ecurity **O**fficer, a leadership function in cybersecurity and one of the ECSF profiles.
CISSP	**C**ertified **I**nformation **S**ystems **S**ecurity **P**rofessional is a certification provided by ISC2 and a well-known course in the cybersecurity industry.
Competence	Demonstrated ability to apply knowledge, skills and attitudes for achieving observable results.
CONCORDIA	EU H2020 project '**C**yber Security C**o**mpete**nc**e f**o**r **R**esearch an**d** **I**nnov**a**tion'.
Course	A series of lessons or a study plan on a specific topic. The duration is minimum 5 hours and participants receive a certificate.
CRA	**C**yber **R**esilience **A**ct is a European regulation that focuses on improving the security of digital products and services.
CTI	**C**yber **T**hreat **I**ntelligence is the process of collecting, analysing, and applying data on cyber threats, adversaries, and attack methodologies.
CVSS	**C**ommon **V**ulnerability **S**coring **S**ystem is a way to evaluate and rank reported vulnerabilities in a standardised and repeatable way.
CyberSec4Europe	European research project aimed at strengthening and consolidating Europe's cybersecurity capabilities.

CyberSecPro	European project and platform that aims to bridge the gap between academic education and practical skills in cybersecurity.
CYTIM	**CY**bersecurity **T**raining **I**nitiatives **M**ap, part of the CADMUS-project and -website, shows database of educational offerings.
DevSecOps	**Dev**elopment, **Sec**urity, and **Op**eration**s** is an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.
DNS	**D**omain **N**ame **System** is a system that turns domain names into IP addresses, which browsers use to load internet pages.
DOM	**D**ocument **O**bject **M**odel connects web pages to scripts or programming languages by representing the structure of a document.
DORA	**D**igital **O**perational **R**esilience **A**ct is a regulation introduced by the European Union to strengthen the digital resilience of financial entities.
e-CF	European **e-C**ompetence **F**ramework provides a reference of 41 competences as applied at the Information and Communication Technology (ICT) workplace, using a common language for competences, skills, knowledge and proficiency levels that can be understood across Europe.
ECHO	**E**uropean network of **C**ybersecurity centres and competence **H**ub for innovation and **O**perations aims to strengthen the European Union's cyber defence through cooperation between different sectors and domains.
ECSF	**E**uropean **C**ybersecurity **S**kills **F**ramework is a practical tool to support the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals. It is the EU reference point for defining and assessing relevant skills, as defined in the Cybersecurity Skills Academy.
ECTS	**E**uropean **C**redit **T**ransfer and Accumulation **S**ystem is a tool of the European Higher Education Area for making studies and courses more transparent.
Education	Process of facilitating learning or the acquisition of knowledge, skills and competences. It encompasses both formal and informal learning experiences. Duration: minimum 1 year and students receive a formal degree.
Educational offerings	Various forms of instruction and resources provided to enhance knowledge, skills and competences. It includes formal education, courses and trainings.
EHEA	**E**uropean **H**igher **E**ducation **A**rea meant to ensure more comparable, compatible and coherent higher education systems in Europe.
ENISA	European Union Agency for Cybersecurity is the EU agency dedicated to enhancing cybersecurity in Europe.
ESCO	**E**uropean **S**kills, **C**ompetences, Qualifications and **O**ccupations is the European classification of Skills, Competences and Occupations relevant for the EU labour market, education and training. It is cross-sectoral and not work domain specific.
EQF	**E**uropean **Q**ualification **F**ramework, standard for education level (values 1..8), top 5 levels directly linked to e-CF levels (1..5).

EU	**E**uropean **U**nion
GDP	**G**ross **D**omestic **P**roduct is the standard measure of the value added created through the production of goods and services in a country during a certain period.
GDPR	**G**eneral **D**ata **P**rotection **R**egulations sets out detailed requirements for companies and organisations on collecting, storing and managing personal data.
GIAC	**G**lobal **I**nformation **A**ssurance **C**ertification is an information security certification body founded in 1999 by the SANS Institute that provides vendor-neutral, technical certifications to validate the specialised skills and knowledge of cybersecurity professionals.
ICS	**I**ndustrial **C**ontrol **S**ystems are integrated hardware and software configurations used to control and automate industrial processes.
ICT	**I**nformation and **C**ommunication **T**echnology is the infrastructure and components that enable modern computing.
IoT	**I**nternet **o**f **T**hings is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud.
ISACs	**I**nformation **S**haring and **A**nalysis **C**entres are non-profit, trusted hubs designed to improve cybersecurity resilience across critical sectors by enabling the collection, analysis, and secure exchange of threat information between public and private stakeholders.
ISMS	**I**nformation **S**ystem **M**anagement **S**ystem is the name for policies and procedures that enable organisations to systematically manage information security.
IT	**I**nformation **T**echnology is the use of computers and other electronic devices to store, retrieve, transmit, and manage data.
LLMs	**L**arge **L**anguage **M**odel(**s**) is an advanced AI technology focusing on understanding and analysing text.
LMS	**L**earning **M**anagement **S**ystem is a software application used for planning, delivering, and tracking training and educational programmes.
LOS	**L**earning-**O**utcome **S**et(s) is a concise description of what students will learn and how that learning will be assessed.
LOTL	**L**iving **O**ff **T**he **L**and is a fileless malware cyberattack technique where the cybercriminal uses native, legitimate tools within the victim's system to sustain and advance an attack.
LOTS	**L**iving **O**ff **T**rusted **S**ites is a cyberattack technique where malicious actors leverage the well-earned credibility and reputation of legitimate, trusted sites and exploit them to carry out their illicit activities.
MFA	**M**ulti-**f**actor **A**uthentication is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
ML	**M**achine **L**earning is the process of training a piece of software, called a model, to make useful predictions or generate content (like text, images, audio, or video) from data.
NERO	Adva**N**ced cyb**E**rsecurity awa**R**eness ec**O**system is a European project that aims to increase cybersecurity awareness among small and medium-sized enterprises (SMEs).

NIS2	**N**etwork **I**nformation **S**ecurity2, Directive (EU) 2022/2555.
OT	**O**perational **T**echnology is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.
Public professional	A professional who works within a governmental organisation or public institution, such as ministries, municipalities or the police. These individuals are usually responsible for national, regional, or sector-specific policy development, oversight or public task execution.
REWIRE	Project Cybersecurity Skills Alliance addresses the skill gaps and shortages in different occupational profiles and qualifications of the Cybersecurity Sector.
SaaS	**S**oftware **a**s **a S**ervice is a cloud-based software delivery model in which providers host applications and make them available to users over the internet. SaaS users typically access applications by using a web browser or app.
SBOM	**S**oftware **B**ill of **M**aterials is a comprehensive list of all the software components, dependencies, and metadata associated with an application.
SCADA	**S**upervisory **C**ontrol and **D**ata **A**cquisition is an architecture that enables industrial organisations to manage, monitor and control (processes, machines and plants).
SD	**S**tandard **D**eviation is a statistical measure that quantifies the amount of variation or dispersion of a set of data values around its mean (average).
SecOps	**Sec**urity **Op**eration**s** is the practice of managing and maintaining an organisation's security posture through a combination of people, processes, and technology.
SG&TTX	**S**erious **G**ames & **T**able-**T**op E**x**ercises.
Skill	Ability to perform an action competently.
SME	**S**mall and **M**edium **E**nterprise; engaged in an economic activity with a limited number of employees (1 to 250), turnover and balance sheet as well as resources. SMEs can encompass (cybersecurity) startups, training businesses, IT/OT/cybersecurity-dependent SMEs (industry professionals) and others.
SOC	**S**ecurity **O**perations **C**entre is a centralised team and facility that monitors, detects, analyses, and responds to cyber security threats against an organisation's IT infrastructure.
SOHO	**S**mall **O**ffice/**H**ome **O**ffice refers to small professional businesses that are often run out of homes, or even virtually.
SPARTA	**S**trategic **P**rograms for **A**dvanced **R**esearch and **T**echnology in Europe is a European project that aims to review and improve cybersecurity research, innovation, and training in Europe.
STEM	STEM is an umbrella term that groups **S**cience, **T**echnology, **E**ngineering and **M**athematics education that promotes the development of foundational competences and transversal skills such as problem-solving, critical thinking, and collaborative skills, laying the groundwork for innovative education in the subjects above.

Training	A form of learning in which you acquire or improve new skills, knowledge, or behaviour under supervision. The duration is 1 to 5 hours and participants receive a participatory certificate.
TTPs	**T**actics, **T**echniques and **P**rocedures is a framework used to understand how attackers operate, what strategies and techniques they use, and what procedures they follow to achieve their goals.
UCD	**U**ser-**C**entred **D**esign is an iterative design process in which designers focus on the users and their needs in each phase of the design process.
UI	**U**ser **I**nterface is the point of communication between a person and a machine.
VA	**V**ulnerability **A**ssessor is someone who define, identify, classify and prioritise vulnerabilities in computer systems, applications and network infrastructures.
VET	**V**ocational **E**ducation and **T**raining
VPN	**V**irtual **P**rivate **N**etwork describes the opportunity to establish a protected network connection when using public networks.
WCAG2.1	**W**eb **C**ontent **A**ccessibility **G**uidelines **2.1** defines how to make web content more accessible to people with disabilities.
WP	**W**ork **P**ackage, part of the CADMUS project.

EXECUTIVE SUMMARY

"The CADMUS project contributes to the overall Digital Europe Programme objectives by enhancing the quality and effectiveness of cybersecurity training across Europe, ensuring that training and education frameworks are developed, data are aligned with both current and emerging cybersecurity needs" (CADMUS, 2025a). The aim of the CADMUS project and this report are: reinforcing the overall CyberSecurity Skills Academy initiative and contributing to a unified European framework for action in cybersecurity skill development. CADMUS's contribution includes the development of curricula, training platforms and training delivery, based on identified skill gaps in Dutch, Greek, Cypriote and Croatian labour markets, amongst others.

Work Package 2 of CADMUS focuses on the unique challenges and risks faced by Small and Medium Enterprises (SMEs) and the public sector, identifying competence gaps and defining training specifications as emerging from the gaps and developments such as new standards and regulations (Network and Information Security Directive 2 (NIS2), Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA)), domain-specific trends (e.g. adoption of cloud and hybrid platforms & automation and AI in security operations) and the increase in complex and sophisticated (cybersecurity) threats. In this deliverable (D2.1), the labour markets from three of the participating countries are analysed in high detail and seven other European Union (EU) country analyses are used to validate and extent the applicability of findings for future upscaling. A total of eight different methods is used to gain insights in the current- and future labour market, educational offerings and to estimate the gap between them. Each country has differing key findings:

Netherlands

The Dutch cybersecurity labour market shows that is requires high qualification and competency expectations of its workforce. The majority of job postings require candidates to possess at least a bachelor- and/or master-level education. The top five most frequently classified competences in vacancies of the Dutch labour market are 'B.1. Application/Product Development', 'C.4. Problem Management', 'D.7. Science and Analysis', 'D.12. Security Consulting' and 'E.4. Relationship Management'. More specifically, Dutch SMEs regularly offer specialised cybersecurity expertise to their clients, which highlights the importance of competences 'D.12. Security Consulting' and 'E.4. Relationship Management', in combination with stronger capabilities in the Build and Run type competences ('B.1. Application/Product Development', 'C.4. Problem Management', 'C.5. Systems Management'). Dutch public professionals demand a significant number of competences that are of use in strategic decision-making ('A.7. Technology Trend Monitoring', 'D.7. Science and Analysis', 'D.12. Security Consulting', 'E.4. Relationship Management') and maintain a partial need for technical competences ('B.1. Application/Product Development')

Cybersecurity programmes in the Netherlands, spanning both public and private educational offerings, emphasise a well-rounded set of core competences aligned with industry needs. The most prevalent competences are 'E.8. Information Security Management', 'E.3. Risk Management', 'B.3. Testing', 'E.6. Quality Management and Compliance', 'C.5. Systems Management' and 'C.4. Problem Management', all of which support the operational and regulatory aspects of cybersecurity. More specialised topics such as 'D.7. Science and

Analysis', 'A.5. Architecture Design' and 'A.7. Technology Trend Monitoring' are also represented, indicating a forward-looking approach that prepares learners for evolving technological landscapes.

Greece

The ICT Service Management labour market sector demands skills such as data analysis, data privacy, incident management, cloud security, information systems & network security, access controls & identity management, threat analysis and problem solving. Greece training offerings focus highly in Security Consulting, Risk Assessment and Management along with consulting roles, while Architecture design and Testing and Engineering are only provided in few courses.

There is a misalignment between cybersecurity training supply and demand in the Greek labour market. Despite some positive developments in postgraduate education and non-formal training, entry-level gaps, limited professional certification uptake, and low awareness among employers hinder effective workforce preparation. A strategic alignment between education, certifications, ECSF roles, and employer needs is essential.

To tackle the demand, training strategies such as upskilling existing ICT personnel, on-the-job coaching and training, in-company training by external providers, reskilling non-ICT personnel and in-company training by own staff are deemed most effective.

Cyprus

The Cypriote labour market shows a strong demand for professionals with solid operational expertise and the ability to work independently. Senior-level roles remain less common, reflecting the national cybersecurity ecosystem's relatively small scale and developing maturity. The top five most classified competences within the vacancies of Cypriote labour market are 'A.7. Technology Trend Monitoring', 'B.5. Documentation Production', 'C.4. Problem Management', 'D.7. Science and Analysis' and 'D.12. Security Consulting'. More specifically, SMEs prioritise professionals who can build, test, and maintain secure systems. The emphasis on 'B.3. Testing' and 'A.5. Architecture Design' reflects the need for robust system development and deployment capabilities. 'E.3. Risk Management' and 'C.4. Problem Management' further underscore the importance of operational continuity and incident response in resource-constrained environments. Public professionals show a strong demand for strategic, analytical, and advisory competences ('A.7. Technology Trend Monitoring', 'B.4. Solution Deployment', 'B.5. Documentation Production', 'C.4. Problem Management', 'D.1. Information Security Strategy Development', 'D.3. Education and Training Provision', 'D.7. Science and Analysis', 'D.12. Security Consulting').

The Cypriote cybersecurity programmes reflect a growing awareness of the need to build national cybersecurity capacity, though the scope and depth of competences ('A.7. Technology Trend Monitoring', 'B.6. ICT Systems Engineering', 'D.1. Information Security Strategy Development', 'E.3. Risk Management' and 'E.9. Information Systems Governance') addressed vary significantly across programmes of study. The majority of training is provided at intermediate proficiency levels, which corresponds to roles requiring the ability to apply cybersecurity concepts independently in real-world settings.

Croatia

Within the Croation labour market most job postings indicate a distinct preference for experts capable of independent operation with specialised knowledge. The Croatian market prominently prioritises operational and implementation-focused roles ('B.5. Documentation Production', 'C.4. Problem Management'). Nonetheless, planning and enabling domain competences are becoming increasingly prevalent, particularly in government-related positions ('D.1. Information Security Strategy Development', 'D.12. Security Consulting', 'E.3. Risk Management' & 'E.8. Information Security Management'). In particular, SMEs have a significant demand for skills in system administration, documentation, operational troubleshooting, and external consultancy ('B.5. Documentation Production', 'C.4. Problem Management', 'C.1. User Support', 'C.5. Systems Management', 'D.1. Information Security Strategy Development', 'D.12. Security Consulting'). The recurrent presence of consulting and risk-related competences suggests that SMEs rely on adaptable expert advice to tailor security solutions to various customer contexts. Public professionals are distinctly focused on governance, strategic supervision, risk management, and instructional responsibilities ('B.5. Documentation Production', 'D.1. Information Security Strategy Development', 'D.3. Education and Training Provision', 'D.4. Purchasing', 'E.2. Project and Portfolio Management', 'E.3. Risk Management', 'E.8. Information Security Management'). Government organisations seek experts who can provide policy guidance, manage risk, oversee extensive projects, and facilitate the effective dissemination of institutional knowledge, rather than those focused solely on hands-on technical implementation.

The examination of cybersecurity education, course and training provisions reveals a robust framework for cultivating technical and operational competences through formal education programmes ('B.1. Application/Product Development', 'C.5. Systems Management'). These programmes are specifically intended to equip professionals for positions centred on implementation, systems management, and information security operations, aligning with the mid-level proficiency spectrum ('D.7. Science and Analysis', 'E.8. Information Security Management'). Nonetheless, a significant deficiency exists in programmes targeting advanced strategic competences, particularly those associated with planning, governance, compliance, and innovation.

ECSF roles

The conducted analysis finds that the 12 ECSF roles are built on a solid foundation of competences, though several competency levels do need refinement in some ECSF roles, to align better with the current vacancies. Examples are that Cyber Incident Responders vacancies often require 'C.4. Problem Management' at level 3, while the role definition mentions level 4, and Cyber Security Researchers are searched for with 'A.7. Technology Trend Monitoring' level 4, while the role definition mentions level 5. Some role definitions matching with vacancies could benefit from adding or removing a competence, for instance adding 'D.7. Science and Analysis' level 3 to Digital Forensics Investigator and removing 'B.3. Testing' from the Cybersecurity Architect role. Despite limitations in the size of the data set and consistencies in labelling of competences, the data suggests support for the creation of three new ECSF roles: *Security Governance Manager, Compliance Officer,* and *Threat Innovation Analyst*.

Gaps and opportunities for training material development
The five most important opportunities for expanding the educational offerings are the competences 'D.3. Education and Training Provision', 'D.9. Personnel Development', 'C.4. Problem Management', 'D.1. Information Security Strategy Development', and 'E.3. Risk Management'. For these competences, the expected demand exceeds the current supply of educational offerings. The gaps suggest that the main priority for new development of training is not necessarily on technical competences, but rather the strategic and business-oriented ones. However, when breaking down the data by level, we observe that 'C.4. Problem Management', 'C.5. Systems Management', 'B.3. Testing', 'E.3. Risk Management', and 'E.6. Quality Management and Compliance' also rank among the most significant gaps. This data highlights the necessity of taking a level-specific approach when determining where to invest in new educational offerings.

The comparison between SMEs and public professionals shows that among SMEs, the three most sought-after competences are 'D.12. Security Consulting', 'C.5. Systems Management', and 'C.4. Problem Management'. In contrast, large public organisations primarily emphasise 'D.12. Security Consulting', 'D.7. Science and Analysis', and 'E.4. Relationship Management'. Furthermore, evidence from other European studies suggests that SMEs tend to prefer informal learning methods and short-term training programmes.

Based on the analysed data sets for educational items, an online database has been designed and built. Visitors can use the website for selecting the best education, course or training depending on their ECSF role, specific competence need and country- or topic preference. There are offers for both starting talents as well as more seasoned professionals. The online database also provides data-driven evidence, with visual aids, to identify missing roles, missing competences and under-served countries which can be used to support recommendations for new Learning-Outcome Sets (LOS) and consequent training initiatives.

A roadmap for training development with LOS (training requirements for 24 components) has been developed: it outlines current deficiencies, forecasts impending legislative and technological challenges, and provides curriculum designers with a framework for tiered, interoperable training modules in later stages of the project. Based on the identified gaps, multiple LOS are proposed, which function as starting point for the development of new trainings. For example, for 'D.3. Education and Training Provision' the LOS 'Cyber-Education & Training Toolkit' is set up. In practice, this entails a recommendation for a Mentor-guided design studio (Learning Management System). Similarly, for 'E.3. Risk Management' a LOS recommendation is to develop a blended micro-credential and workshop on Key Risk Indicators.

1 INTRODUCTION

This deliverable produced within the European Union (EU) co-funded CADMUS project analyses cybersecurity training needs for Small and Medium Enterprises (SMEs) and public administrations. The analysis combines evidence from recent job vacancies, the current landscape of education and training opportunities, and comparative needs assessments conducted in several EU Member States. It also incorporates trend analysis and focus group results to identify emerging competence requirements. This is the basis for the included Cybersecurity Training Initiatives Map (CYTIM) and training requirements specifications. It aligns with CADMUS's goals for developing curricula, training platforms and training delivery (work packages 3, 4 and 5).

Work Package 2 (WP2) focuses on the unique challenges and risks faced by SMEs and the public sector, identifying competence gaps and defining training specifications as emerging from the developments related to regulatory tightening, technical developments, and security and risk changes. Current and previous EU projects have mainly focused on utilising job profiles and formal standardised job descriptions of cybersecurity experts to identify needs stemming from SMEs and the public sector. Illustrative is the utilisation of titles and/or overall descriptions from job vacancy advertisements, labelling based on keyword counting or verbatim European Cybersecurity Skills Framework (ECSF) profiles which are used as labels without further detailed mapping of underlying needs. CADMUS equips another approach to identify cybersecurity competency demand and supply, and applies this to the Netherlands, Croatia and Cyprus. The method can easily be applied to other European job markets or specific sectors. CADMUS facilitates the development of targeted, relevant and practical cybersecurity training programmes that are aligned with real-world SME and public sector demand. Each country collects a set of vacancy descriptions (competency demand) and educational listings (competency supply); labels each identified and relevant competence within the vacancy description or educational listing according to the modified e-Competence Framework (e-CF) which provides input for the countries' current needs analyses and counts the competences overlap with the current twelve roles from the ECSF. This data is validated through several focus groups, additionally analysed available countries reports and supplemented by trend analyses to include expected future needs.

Follow up activities in WP2 include the detailed specification and training plan (Deliverable 2.2), updates of the needs analysis based on new vacancies and available trainings, and alignment with the Cyber Security Skills Academy (Deliverable 2.3).

1.1 Scope

Our analysis focusses on competences as the more stable element for human development, instead of, for instance, specific knowledge areas. In practice, we use a predefined and widely recognised and applied competence framework, namely the e-CF, that is also one of the core elements of the ECSF. A competence is a demonstrated ability to apply knowledge, skills and attitudes for achieving observable results (European Commission, 2025a). Unlike knowledge or

skills alone, competences are not domain or application specific, making them more transferable and enduring across different contexts.

We analyse labour and education markets from three of the participating countries in high detail and on seven other countries available studies to validate applicability for future upscaling of trainings. It is possible, although deemed not very likely, that there are certain countries or areas for application of the analysis method that require further detailing or splitting up competences.

Education and training are used interchangeably unless otherwise specified. This includes training through the mentioned methods of cyber ranges, online training, serious games, tabletop exercises, bootcamps and hackathons. We limit the scope to recurring training and education, not one-time events. These also need to be accessible for other professionals or organisations, not in-company training for instance. The trainings need pre-defined learning outcomes to be included; this allows for competence classification and selection beforehand instead of ad-hoc peer learning sessions or community gatherings without a pre-defined learning objective.

Our focus is not sector specific. We do however target two very different and distinct groups: employees working in SMEs and public professionals. Analyses are made specific for these groups. While it is expected that the analyses' findings show overlaps with other types of organisations, such as big industries and research organisations, these are not the focus of this deliverable.

1.2 Target groups

There are several target groups for which this deliverable is relevant. They are:

- The developers of training material in the CADMUS project (mainly WP3).
- Policy makers on cybersecurity and labour/education market, including educators, trainers and capacity builders as developers. The most prominent are those that are involved with the needs of SMEs and public professionals.
    - In general, an **SME** is an enterprise engaged in an economic activity with a limited number of employees (1 to 250), turnover and balance sheet as well as resources (European Union, 2020). SMEs can encompass (cybersecurity) startups, training businesses, Information Technology (IT)/Operational Technology (OT)/cybersecurity-dependent SMEs (industry professionals) and others.
    - **Public professionals** work within a governmental organisation or public institution, such as ministries, municipalities or the police. These individuals are usually responsible for national, regional, or sector-specific policy development, oversight or public task execution. Public professionals can encompass cybersecurity and IT policy makers, civil IT procurement specialists, cybersecurity specialists and system administrators within public employers.
- Interested members of similar projects (amongst other from the Digital Europe Programme including the call from which this project is co-funded), labour- or education market analysts and scholars on this topic.

The target groups for the resulting training that is to be developed within CADMUS (end users) are:

- **Employees within SMEs**, these can be in full time cybersecurity roles or just have cybersecurity activities as one of their tasks.
- **Employees within public authorities, services and institutions**, these can also be in full time cybersecurity roles or just have cybersecurity activities as one of their tasks.
- **Educators, Trainers, and Capacity Builders as learners.** Educators, trainers and capacity builders are key stakeholders in attaining scalable cybersecurity education across all skills levels and competence fields. These stakeholders (e.g. academic staff, vocational trainers and corporate learning managers) are responsible to deliver engaging and standards-aligned cybersecurity training and reskilling programmes for a wide variety of audiences. They therefore need access to learning material for their own continuous development.
- **Students and Early-Career Pursuers.** Science, technology, engineering and mathematics (STEM) and other graduate students, vocational trainees and emerging cybersecurity professionals are new to the cybersecurity field and require significant training to develop their capacities.
- **Career Changers, Reskilling Candidates, and Lifelong Learners.** Career changers, lateral entrants, reskilling candidates and lifelong learners are stakeholders that either move from a particular field to the realm of cybersecurity or re-enter the cybersecurity workforce in a different field. They may overlap with one of the two first groups (employees of SMEs or public employers).
- **Under-represented Groups**
  Learners from underrepresented groups in the cybersecurity domain are for example women from rural populations, those individuals with limited financial resources or individuals with learning disabilities. They may overlap with all earlier mentioned groups.

1.3 Training & education systems

The context in which the aforementioned target groups develop is important to be aware of. It is outside the scope of the CADMUS project to change or impact these, nonetheless they are of influence for the rollout and adoption of developed trainings and therefore mentioned here.

1.3.1 Adult education & lifelong learning

Adult education and lifelong learning opportunities vary significantly across Europe. Northern European countries generally provide better-developed systems for continuous learning, including micro-credentials and subsidised training schemes for employed adults (European Commission, 2022a). By contrast, in several Southern and Eastern European countries, adult education remains fragmented and underfunded, making it harder for employees, especially in SMEs, to access high-quality, short-term cybersecurity upskilling or retraining. The percentage of employees that follow learning programmes or courses varies across member states (Eurostat, 2024). These structural and cultural differences emphasise the need for easily accessible, adaptable, practice-oriented cybersecurity training initiatives that align with the diverse training- and education systems across Europe.

1.3.2 European education systems

European education systems are characterised by a strong distinction between general education, vocational education and training (VET), and higher education. In countries such as Germany, Austria, and Switzerland, VET is deeply rooted in a dual system where learners alternate between classroom-based learning in vocational schools and practical on-the-job training with employers. This structure ensures high labour market relevance and a smooth school-to-work transition (Cedefop, 2020). In contrast, countries in Southern and Eastern Europe often rely on school-based vocational education with limited workplace training components, leading to weaker links between vocational pathways and employers (European Commission, 2022b).

1.3.3 Higher education

Higher education in Europe includes academic pathways (universities) and professional-oriented higher education (Universities of Applied Sciences or polytechnics). In many countries, universities focus on theoretical and research-oriented education, while universities of applied sciences combine practice-based teaching with professional skills development (European Commission, 2025b). For instance, in the Netherlands, Universities of Applied Sciences ("hogescholen") offer professionally oriented bachelor's degrees with strong links to industry, whereas research universities provide more academically focused programmes (PTvT/Dialogic, 2024).

All countries involved in this project are members of the European Higher Education Area (EHEA)[1] and therefore party to the European Cultural Convention[2] and declared their willingness to pursue and implement the objectives of the Bologna Process in their own systems of higher education. The Bologna Process' key principles are harmonising degree structures through a three-cycle system, European Credit Transfer and Accumulation System (ECTS) credits, and quality assurance, while enhancing mobility, recognition, inclusivity, and lifelong learning to create a cohesive EHEA.

1.3.4 Cybersecurity training market

At the same time, the cybersecurity professional training market has been present in most countries before formal programmes at different schools became available for this subject. Well known certifications and training providers determine the market for professionals more than educational institutes. Vacancy analyses show that certification requirements (such as CISSP, CISM, CISA, see for instance PTvT/Dialogic, 2024) are encountered more frequently than formal education requirements in cybersecurity (such as a 'Bachelor in Cybersecurity'). The sheer amount and diversity of offers and limited structure across certifications, except for those provided by the same issuer, can be overwhelming. A lack of structure and overview in cybersecurity training and education can hinder both employers and (future) professionals.

[1] https://ehea.info/index.php

[2] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=018

1.4 Readers' guide

Chapter 2 describes the used methodologies for the quantitative analysis of the labour market needs based on job vacancies, the education market offerings and the qualitative analysis of the literature review on trends and developments, the use of focus groups and the competence gap analysis.

Chapter 3 describes the recent labour market needs in the Netherlands, Cyprus and Croatia with highlighted differences between SMEs and public professionals. For each of these countries there are insights in the labour market demand, the most in demand competences and the mapping to ECSF profiles. To get a more complete overview of needs in Europe, we also analysed relevant existing reports about seven other European countries. The chapter concludes with an overall conclusion of labour market needs and possible new or adjusted ECSF roles based on labour market data.

Chapter 4 identifies and assesses trends that are expected to impact the need for cybersecurity competences. The existing need for cybersecurity competences and underlying skills within SMEs and public sector stemming from several EU co-funded cybersecurity labour market projects are analysed. There is also a review of broader developments that may impact the cybersecurity field of work based on publicly available in reports and studies. These cover topics such as EU-legislation, technical developments and emerging risks. An assessment of expected future cybersecurity needs is based on them. Results from several focus groups sessions that were held in the first half of 2025 with public sector, business and education experts are included. The chapter concludes with a summary of expected future needs based on the three different sources in this chapter.

Chapter 5 provides an insight into current education-, courses- and training offerings per partner country based on the competence framework also used for vacancies and trends. Additional insights from other studies regarding offers for development of competences and skills are presented. This chapter concludes with an overall analysis of current offerings.

Chapter 6 combines the insights from chapters 3, 4 and 5 for a Gap analysis per partner country and an overall analysis based on the difference between labour market current and expected future needs, and current educational offerings.

Chapter 7 describes the design for a Cybersecurity Training Initiatives Map (CYTIM). The functional and technical requirements for visualisation are described. The resulting CYTIM visualisation is presented as the conclusion of this chapter.

In chapter 8 the report specifies competence-based training requirements and underlying learning objectives which will be further detailed in deliverable 2.2 and developed within CADMUS.

2 METHODOLOGIES

A multi-layered methodological approach is utilised to come to a thorough competence gap analysis. In turn, the gap analysis provides input and insights for the development of tailored-made trainings and courses through training requirements. The collected education, courses and trainings are shared on the project website. The vacancy analysis is the basis for reflecting on current and potential new ECSF roles.

In this chapter, the methodology for collection, competency labelling of vacancy descriptions and educational offerings through the adjusted e-CF and matching with ECSF roles is explained first. Second, the methodology for labour- and education market data analysis is laid out. Third, the further analysis of ECSF roles based on the vacancy analysis is described that will lead to suggestions for further development of the current 12 defined roles. Fourth, the method we used for country report analysis for seven EU countries is described. Fifth, the literature analysis of previous EU-projects and relevant trends (sixth) is methodologically outlined. In the seventh paragraph, the set-up of the focus groups is highlighted. Lastly, each component is utilised in the gap analysis, determining the difference in expected future competence need and current offers for development of competences. For an overview of the relations between data collections, methods (with reference to the paragraph where the methodologies are described in more detail) and results, see Figure 1.

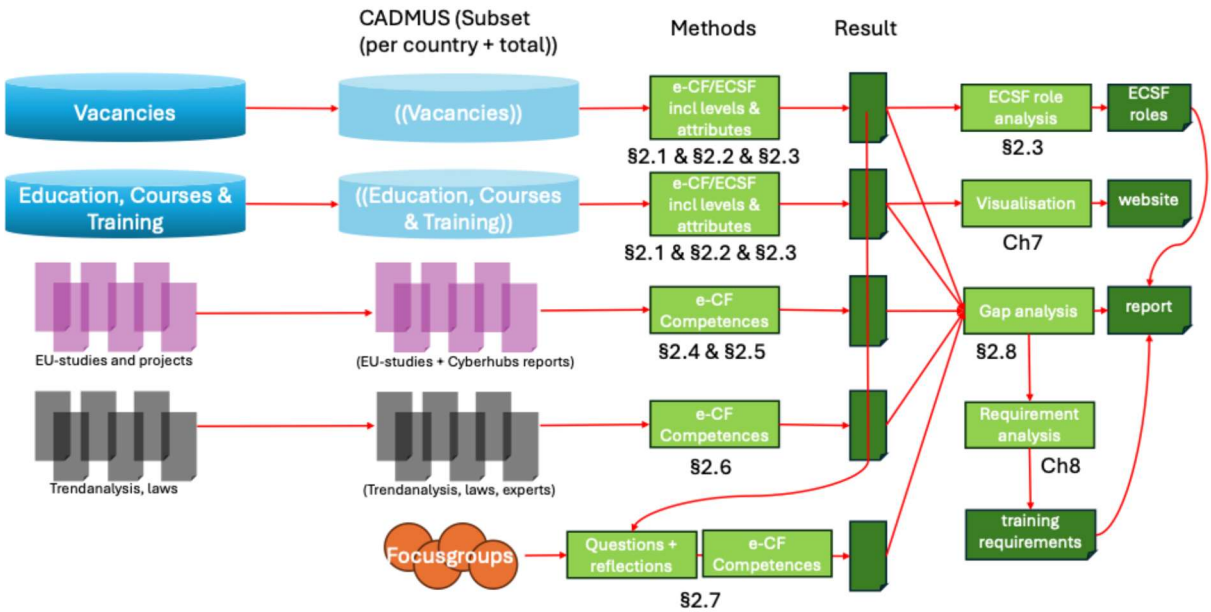

Figure 1: Schematic overview of data sources, applied methods and results as applied in this study with references to paragraphs and chapters with method descriptions.

2.1 Labelling vacancies & educational offerings

The first step towards the labelling of vacancy descriptions and educational offerings is the collection process. Vacancies and educational offerings are collected via various means. For example, for the Netherlands vacancy databases (HSD's securitytalent.nl) and the Dialogic education database selection (PTvT/Dialogic, 2024) are used. Other countries utilise web search tools in which queries are used to obtain relevant vacancies and educational offerings or previously constructed project databases. For the CADMUS project, vacancies and educational offerings that are directly impacting cybersecurity work have been included.

Accurately labelling the text of a job vacancy or educational offering with relevant competences is a vital step towards creating an accurate database that provides the basis for properly analysing the labour markets of countries. This process goes beyond simply identifying required skills—it involves linking specific phrases or tasks in the text to the adjusted set of e-CF competences. We make use of this adjusted set previously developed and used by HSD (including practical examples), instead of the original e-CF definitions, to better fit with cybersecurity and make labelling more coherent. The original and adjusted e-CF definitions also function as input for the development of ESCO (European Skills, Competences, Qualifications and Occupations, European Commission, 2024). A more detailed overview of the labelling process and how to avoid common pitfalls is included in Annex 1. Annex 2 Example vacancy labelling based on e-CF includes an example illustrating how a vacancy text is labelled with competences, the same can be applied to a description of an educational offer. Sections describing personal characteristics, general organisation description, or the application procedure are usually excluded. Personal characteristics and acquiring a certain type of knowledge are not considered to be competences but can be combined into one. In Annex 3 Step-by-step guide for labelling vacancies with competences, a step-by-step guide can be found on how to label texts with competences. Annex 4 and Annex 5 provide further insights into the types of factors that have been taken into account when labelling vacancy descriptions (Annex 4) and educational offerings (Annex 5).

There are some limitations in the collection and classification of datasets for vacancies and educational items.

- Differing datasets per country (not standardised and data input differs) and differing methodologies (some vacancy analyses have been conducted through surveys instead of data-driven textual analysis).
- The labelling process is prone to biases (each person labels slightly different) and labelling is carried out on the texts as given but these can be ill defined (individual words do not provide enough context to describe competences accurately; paragraphs may include several competences without sufficient distinction) or don't describe the actual job very well.

Differences in vacancy and educational offerings datasets from non-complete data and the subsequent use of differing methodology can lead to alternate results that are not representative for all the participating countries. We deem vacancy and training texts as the most realistic sources when it comes to identifying labour market demand and educational offerings across big volumes. Through providing an e-CF manual how to label and classify competences there has been coordinated guidance during the process between the partners.

By going through current vacancies from partner countries together and discussing the chosen competences, there is more consistency in interpretation, and it narrows down fixed biases. Since we combine the data for the gap-analysis and not use it for individual employee, employer of training provisioner, we expect the emerging gaps to be robust for smaller measurement errors.

2.2 Labour- and education market data analysis

Countries deliver data for the tables mentioned below based on the previous paragraph. This provides a solid foundation from which the country analysis is conducted. After each country analysis, the findings are synthesised into two coherent summarisations, one for vacancies and one for educational offerings (see Annex 6 for the tables per country, the main results are presented in '3.1 Current labour market needs' and '5.1 Current education, course & training offerings'). This provides insights into current needs and offerings in the cybersecurity labour markets.

Each vacancy or training programme offers competences that can align with ECSF profiles. The combination of competences results in a percentage score for the degree of overlap with the ECSF profile definition. Elements of multiple profiles are in practice often combined in a single vacancy. The average match percentage indicates the required profiles. The standard deviation (SD) serves as a supplementary measure. The number of vacancies or programmes where the position in question has the 1st, 2nd, or 3rd highest score level of match is shown in the last three columns (see different tables in Annex 6).

The basis for the analysis is:

1. Seven tables of data per country for vacancy analysis:
   a) Number of competences with proficiency level (1-5) present within total number of vacancies.
   b) Percentual comparison of labelled competences within total number of competences & percentual comparison of competences present within total number of vacancies.
   c) Number of competences with proficiency level (1-5) present within SME vacancies.
   d) Percentual comparison of labelled competences within total number of SME competences & percentual comparison of competences present within SME vacancies.
   e) Number of competences with proficiency level (1-5) present within public professional vacancies.
   f) Percentual comparison of labelled competences within total number of public professional competences & percentual comparison of competences present within public professional vacancies.
   g) Percentual match of ECSF roles within vacancies, its standard deviation and the number of vacancies where the mentioned role is the number 1st, 2nd or 3rd highest scoring level of correspondence.

2. Ten tables of data per country for educational analysis:
   a. Number of competences with proficiency level (1-5) present within total number of trainings, courses and education offerings.

b. Percentual comparison of labelled competences within total number of competences & percentual comparison of competences present within total of trainings, courses and education offerings.
c. The number of competences present within the total number of trainings, courses and education offerings that are classified either as class, online or hybrid & the percentage that a competence is available in the total number of trainings, courses and education offerings in this classification (class, online, hybrid).
d. Number of competences with proficiency level (1-5) present within education offerings.
e. Percentual comparison of labelled competences within total number of education offerings competences & percentual comparison of competences present within education offerings.
f. Number of competences with proficiency level (1-5) present within courses.
g. Percentual comparison of labelled competences within total number of course competences & percentual comparison of competences present within courses.
h. Number of competences with proficiency level (1-5) present within trainings.
i. Percentual comparison of labelled competences within total number of training competences & percentual comparison of competences present within trainings.
j. Percentual match of ECSF roles within the total of trainings, courses and education offerings, its standard deviation and the number of trainings, courses and education offerings where the mentioned role is the number 1st, 2nd or 3rd highest scoring level of correspondence.

2.3 ECSF roles analysis

An additional objective of this report is to develop and formulate recommendations that contribute to the development of ECSF roles. The ECSF roles are developed by ENISA (European Union Agency for Cybersecurity). The ECSF serves as a "common understanding of cybersecurity professional role profiles, along with clear mappings to the relevant skills and competences required". In other words, it's a tool to unify how we talk about cybersecurity jobs across the EU and support the development of cybersecurity skills (ENISA, 2022a). The ECSF role profiles overlap with the ESCO classification, both frameworks can analyse labour markets in terms of professional roles and required skills. Since "ESCO aims to classify the entire EU labour market across various sectors, while the ECSF provides a focused analysis of role profiles specific to the cybersecurity sector (ENISA, 2025)" we use the latter. If changes are made to the ECSF, these should also translate to changes in the ESCO-database. This is outside the scope of CADMUS.

The methodology of analysing the ECSF roles follows a two-pronged analytical approach. The first approach focuses on competence matching, the Match-based approach. This means that the competences assigned to each vacancy will be matched with the competences assigned to the ECSF role's assigned competences. The higher the match, the closer the vacancy is to the definition of the ECSF role at hand. If this is not the case, the ECSF role is rightfully not a match or should be revised and adjusted to better match the labour market demands. This approach is firstly used to determine the applicability of the ECSF roles to the current labour market.

The second approach, the Name-match approach, bases on hand-picking vacancies with the same or similar name as the to-be analysed ECSF role. This ensures that the vacancy should be a match based on face value, which in turn allows for a more normative approach but still evidence-based comparison of competences with ECSF roles. More details on the method's two elements can be found in Annex 1. Next to the analysis, expert insights from the consortium partners are used to propose potential new roles and adjustments.

2.4 Cyberhubs country analysis

To complement the detailed country analysis with European cybersecurity labour market trends, an in-depth analysis of reports from seven European countries was performed (CyberSecPro, 2024a to 2024h). The analysed countries were Lithuania, Spain, Estonia, Slovenia, Greece, Hungary and Belgium. Their labour market needs that are identified in the reports are mapped to our competence framework, albeit without level indication (there is not enough detail in the reports to make this classification). Sometimes the competences are directly connected to the skills definitions in the reports (data privacy's relation to 'E.9. Information Systems Governance'), in other cases skills are mentioned that combine several competence needs (Incident Management related to 'C.4. Systems Management' and 'E.3. Risk Management'). In total 8 skills needs are related to 10 e-CF Competences, see Annex 6; Tables – CyberHubs. These seven reports collectively served as the primary source material to identify four initial trends. These trends reflected the most prominent developments in the cybersecurity domain.

2.5 Literature review EU projects

A review of existing literature was conducted to examine the current state of the cybersecurity labour market in Europe, focusing on initiatives funded by the EU. The review centres on analysing key outputs and findings from recent EU-funded projects, including CONCORDIA, CyberSec4Europe, CyberSecPro, ECHO, NERO, REWIRE, and SPARTA. Additionally, this study integrates insights from ENISA, particularly its ECSF and the e-CF. For each of the selected EU projects, a range of aspects were systematically examined. These include the overarching goals and objectives of the project and the methodological approaches employed in its execution. This literature review also explores each project's conclusions, outcomes, and key recommendations, with particular attention to how they contribute to understanding or addressing the cybersecurity skills gap in Europe.

Moreover, the literature review considers the development and application of cybersecurity skills frameworks within each project, identifying the specific cybersecurity skills and roles that are in demand across the EU. It further investigates the critical issues currently affecting cybersecurity education and training. Emerging trends and foresight projections related to future skills needs are analysed to provide a forward-looking perspective. Finally, the databases and data sources utilised by the projects to inform their findings and recommendations are identified. By synthesising information across these diverse initiatives, we draw out common themes, best practices, and persistent challenges, contributing to a more integrated and strategic understanding of how the EU can effectively address its cybersecurity workforce

needs. The literature review provides qualitative inputs, such as trends and cybersecurity education developments, which are consequently validated in the focus groups (see Focus groups). The qualitative outputs are mapped to themes, which in term are mapped to one or more competences. This way it is possible that one competence is required for several themes, strengthening its importance for the labour market.

2.6 Trend analysis

A trend analysis was carried out in addition to the literature review. The aim was to translate the insights from the literature review and CyberHubs country reports core trends that would be relevant and recognisable to both the public and private sectors. To achieve this, the findings from the literature review were revisited and supplemented by a renewed analysis of the underlying reports. The analysis focused on clustering recurring themes and key developments in the European cybersecurity landscape. Particular attention was paid to avoiding overlap between the trends. Initially, four provisional trends were formulated. These were tested in a pilot focus group in the Netherlands. Based on the feedback from this session, the trends were refined and reduced to three: EU-legislation, technical developments and security and risk changes. A follow up analysis includes an in depth review of these trends through analysing 20 impactful reports and studies to provide updated insights into these three categories of trends (see '*' in the 'Reference List') . These trends are assessed for expected future cybersecurity tasks and associated competences using the same competence framework as in labelling vacancy descriptions and educational offerings.

2.7 Focus groups

To gather cybersecurity training expectations and to assess cybersecurity skill gaps and workforce needs from various stakeholders, a series of focus groups was organised. We opted for focus groups rather than surveys, for the following reasons:

1. Focus groups allow for more in-depth insights into the perspectives and experiences of experts/participants, especially when dealing with complex or context-specific topics.
2. The interactive nature of focus groups encourages dynamic discussion and the exploration of shared and diverging viewpoints, which helps uncover nuances that are often missed in standardised survey responses.
3. The format allowed real-time clarification and follow-up.

There were three rounds of focus groups, each supported by a facilitator and an analyst for data collection:

1. Pilot focus group (7 cybersecurity professionals from the Netherlands);
2. Employers (one session with 7 cybersecurity representatives of the public sector and one session with 8 cybersecurity professionals of the private sector);
3. Educators (one session with 4 representatives of secondary education and one session with 6 representatives of higher education).

Pilot focus group

The pilot for the focus groups served two main goals:

1. Validate the relevance of initial trends identified through the trend analysis and assess whether experts from both the public and private sector recognised these trends,
2. Validating the methodology and optimising the design for the other focus groups within the CADMUS project.

The pilot focus group consisted of four separate rounds:
1. Cybersecurity developments.
2. Competence gap identification.
3. In-depth discussion on the competence gap.
4. Implications for companies and education.

Methodology - Focus Groups with Employers
Two focus groups with employers were organised: one with representatives from governmental organisations and one with representatives from private organisations/SMEs. Representatives were selected based on several selection criteria including a solid understanding of cybersecurity labour market needs and education (see Annex 7 Results focus groups). The goal of the focus groups was to further specify the cybersecurity developments identified in the trend analysis, as well as the implications for education, government and business.

The focus group consisted of three rounds:
1. Cybersecurity Trends.
2. Key Cybersecurity Competences for the Future.
3. Gap Analysis of Cybersecurity Competences.

A total of 7 representatives from governmental and 8 participants from private organisations participated, evenly distributed across the four participating countries.

Methodology - Focus Groups with Educators
These focus groups explored how cybersecurity education in upper secondary schools and higher education can better meet labour market needs, boost student engagement, and increase the participation of young women. Two focus groups were organised: one with educators/teachers from secondary education and one with educators/teachers from higher education.

The focus groups consisted of three rounds:
1. Gap Analysis of Cybersecurity Competences: Training Offers vs. Job Vacancies.
2. Effective Didactics for Cybersecurity.
3. Empowering Young Women in Cybersecurity Education.

A total of 4 representatives from secondary education and 7 participants form higher education participated, evenly distributed across the four participating countries. The results of all focus groups were coded and analysed by two independent researchers. See ‘Annex 7 Results focus groups’ for the selection criteria and data, and ‘Focus groups’ for their interpretation.

2.8 Competence Gap Analysis

The competence gap analysis aimed to identify discrepancies between current educational offerings and future labour market demands within the cybersecurity sectors in different EU-countries. The methodology employs a multi-layered approach, incorporating market demand data based on vacancy description analyses, market supply data based on current educational offerings, cybersecurity trends and developments distilled through a literature review from previous EU projects, the validation of these trends and developments through focus groups (specialists from public sector, private sector including SMEs and educators), and the identification of cybersecurity developments that may impact competence needs such as legislation, technical developments and changes in risks. The data collection methods for all these are described in the previous paragraphs.

Insights from the literature reviews, trend analysis and focus groups are utilised to adjust the findings of the gap between current vacancies and educational offerings. Therefore, an overall analysis was conducted in which the trends and developments from the trend reports, literature review, and focus groups were linked to the competences they impact. Based on how frequently each trend was identified across these sources, an adjustment factor was applied to determine whether certain competence needs should carry more significance than indicated by the vacancy analysis alone.

The gap analysis is conducted through two approaches: the relative approach and the normative approach. The relative approach, also known as a frequency comparison, is a comparison between educational offerings and job vacancies at the national level. The analysis is done at the proficiency level of individual competences, thereby including a textual description of data limitations and interpretation of results. Extracted data from the relative approach is for example beneficial to provide tailored-made career advice to individuals. For instance, if an individual were to transfer from an Information Security Officer (ISO) role to a Chief Information Security Officer (CISO) role the competence ‘E.8. Information Security Management’ needs to be improved from level 4 to level 5. The identification of the proficiency level gap helps to provide suggestions for courses/trainings that an individual can follow to obtain the required proficiency level.

The normative approach involves the analysis of descriptive values from vacancy descriptions and educational offerings. For example, the study load and study duration can be analysed to identify which education, course or training is best suitable for an individual to follow. Another example can be found in the descriptive value ‘location’. Mapping where educational offerings are can be beneficial for individuals and policy makers, especially in conjunction with the education form (whether an educational offering is online, in class or hybrid) to ascertain where potential gaps are on the regional/national level.

3 NEEDS ANALYSIS

3.1 Current labour market needs

To analyse the labour market needs in the Netherlands, Greece, Cyprus and Croatia it was chosen to conduct research into vacancies, as these show direct demand for employees for different organisations. As described in the methodology the adjusted e-competence framework and the ECSF roles are used. Each vacancy has required e-CF competences embedded in them, which are matched to ECSF profiles. The combination of competences gives a percentual score regarding the size of overlap with each ECSF role. Often elements of several roles are combined in one vacancy. After each individual country's labour market needs are extracted from the analysis, an overarching labour market analysis is conducted to show overlap in competences, roles and needs.

3.1.1 The Netherlands

The starting point of the labour market analysis of the Netherlands is the HSD's Security Talent database. The database contains vacancies within the (cyber)security domain. To align with the scope of Deliverable 2.1, only vacancies that incorporate a cybersecurity component are included in the dataset. The dataset is diverse and unique as a wide array of employers, such as SMEs, large corporate businesses, governmental organisations and knowledge institutions have vacancy postings on Security Talent, dating back as far as 2016. A total of 483 cybersecurity-related vacancies predominantly from the period 2024-2025 have been collected and classified in accordance with the methodology (see Table 1). The classification process has resulted in 1380 competences being extracted from the Dutch vacancies, which amounts to an average of approximately three competences per vacancy (see Table 1).

Vacancy dataset

The 483 Dutch vacancies have the following time distribution: 204 vacancies in 2025; 234 vacancies in 2024; 29 vacancies in 2023; 7 vacancies in 2022 and 9 vacancies in 2021. The focus lies on 2025 and 2024, which are supported by 45 vacancies from three years prior for roles that are rarer. Furthermore, the Dutch labour market shows that it requires or demands high qualification and competency expectations of its workforce. The majority of job postings require candidates to possess at least a bachelor- and/or master-level of work. This finding is reflected through the demand of proficiency level 3 competences (676), closely followed by proficiency level 4 competences (507). Proficiency levels 1, 2 and 5 are demanded significantly less, respectively 7, 126 and 54 times. The strong representation of proficiency levels 3 and 4 can partially be attributed to the relatively high number of postings from corporate businesses (124), knowledge institutions (77) and educational institutions (10). Multinationals, universities and education providers in the Netherlands tend to demand at least a bachelor's or master's degree from its employees in the Netherlands. In particular, knowledge- and educational institutions traditionally offer positions involving academic research, applied innovation or cybersecurity curriculum development for which a higher competence level is essential.

Total vacancies

In Table 2 it is shown that the top five most frequently classified and required competences in vacancies of the Dutch labour market are 'D.12. Security Consulting' (29,81%), 'E.4. Relationship Management' (22,98%), 'D.7. Science and Analysis' (19,67%), 'B.1. Application/Product Development' (14,49%) and 'C.4. Problem Management' (13,87%). There are several explanations and reasons why these competences have a significantly high frequency percentage rate:

- **D.12. Security Consulting**. It is a common practice amongst organisations in the Netherlands to seek (external) expert knowledge or provide expert knowledge to other organisations, for example within the cybersecurity consultancy branch. Governmental institutions in particular, frequently hire external consultants to gain advice on a wide variety of cybersecurity issues. Cybersecurity consultations occur on different levels, ranging from the application of regulatory requirements, such as the Digital Operational Resilience Act (DORA) and Network and Information Security 2 (NIS2), for practical cybersecurity implementations; to expert advise on how to develop a national or local cybersecurity-related agenda or policy.
- **E.4. Relationship Management**. Within the Dutch cybersecurity domain, it is important to be able to communicate and work with a wide variety of internal and external stakeholders. In government positions an individual must often work with different branches within the governmental institution and, frequently, in conjunction with small or large (commercial) cybersecurity providers as well. Similarly, large corporate businesses often have a large portfolio of clients that each have different needs that must be accommodated. SMEs cannot cope with all cybersecurity needs and depend on their suppliers and relations to perform cybersecurity related tasks. Relationship management is therefore a frequently seen competence within Dutch vacancies.
- **D.7. Science and Analysis**. D.7. is a broad competence, encompassing research skills, data science- and analytics skills, and digital forensics skills. Most Dutch research positions require either quantitative or qualitative (data) analysis techniques and skills to translate analysed data into structured (academic) reports. Additionally, vacancies that contain skill components of data analysis, cyber or digital forensics, threat analysis and technical innovation are often classified in accordance with D.7..
- **B.1. Application / Product Development**. B.1. is most often seen within vacancies related to software- or application development. For example, Information and Communication Technology (ICT)- and cybersecurity companies require skilled personnel that can develop and build software or applications for the specialised needs of the organisation. Other companies and organisations focus on developing software and applications for external stakeholders as part of their business model. Because of skills shortages and high salaries employers are trying to automate many cybersecurity tasks.
- **C.4. Problem Management**. C.4. is partially related to B.1. With Dutch organisations digitalizing rapidly, a high competence demand for developing, managing and operating ICT systems and applications is evident. The operational maintenance of ICT systems and applications requires a wide range of problem management skills, from identifying root causes of system and cybersecurity incidents to the provision of effective solutions to maintain production.

SMEs

Of the 483 classified vacancies, 116 are from Dutch SMEs (see Table 3). The most in-demand competences from SME vacancies are 'D.12. Security Consulting' (38,79%), 'B.1. Application / Product Development' (19,38%), 'E.4. Relationship Management' (19,38%), 'C.5. Systems Management' (16,38%) and 'C.4. Problem Management' (15,52%) (see Table 4 & Figure 2). Cybersecurity SMEs need to offer specialised expertise to their clients, which highlights the importance of competences D.12. and E.4.. SMEs typically work with a diverse client base. Within the Dutch cybersecurity sector, SMEs are often responsible for providing cybersecurity software and ICT systems to clients. Moreover, these types of software and systems need continuous updates. ICT systems can for example be externally operated and managed by SMEs which is why they tend to have stronger capabilities in the Build (B) and Run (C) type competences (B.1., C.4., C.5.).

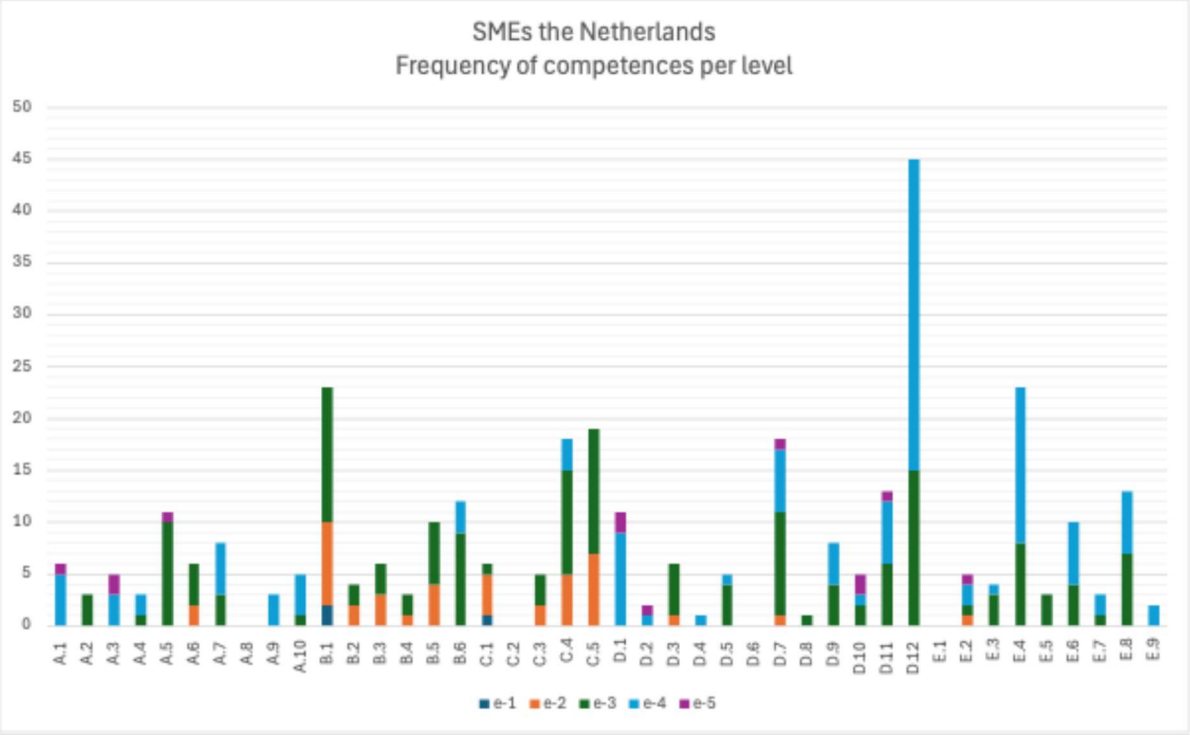

Figure 2. Required competences by SMEs in the Netherlands (n=116).

Public professionals

Of the 483 classified vacancies, 148 are for public professionals, which are often deployed by governmental organisations such as ministries and municipalities (see Table 5). The most in-demand competences from public professionals' vacancies are 'D.12. Security Consulting' (29,73%), 'E.4. Relationship Management' (25,68%), 'D.7. Science and Analysis' (21,62%), 'A.7. Technology Trend Monitoring' (16,89%) and 'B.1. Application/Product Development (11,49%) (see Table 6 & Figure 3). Governmental institutions primarily focus on the e-CF's planning (A), enabling (D) and managing (E) domains of cybersecurity rather than the hands-on implementation of technical measures (Build (B) and Run (C)). There is a partial need for technical competences, highlighted through B.1. (11,49%), C.4. (11,49%) and C.5. (10,14%),

which indicates that Dutch governmental organisations do not want to rely on external business alone for their cybersecurity and ICT systems technical expertise. As an example, the Dutch police develops and maintains systems for their day-to-day operations, instead of externally sourcing the technical expertise. Furthermore, it is logical that the competences D.12., E.4., D.7. and A.7. are the most frequently labelled amongst Dutch vacancies as governmental organisations often include a significant number of internal advisory roles that support higher management in strategic decision-making. D.7. and A.7. are also competences that are required when it comes to developing trend reports and research-based background reports. For example, multiple institutions within the Dutch government provide monthly and yearly updates regarding the Dutch cybersecurity landscape, including technological trends, identified cybersecurity threats and threat actors.

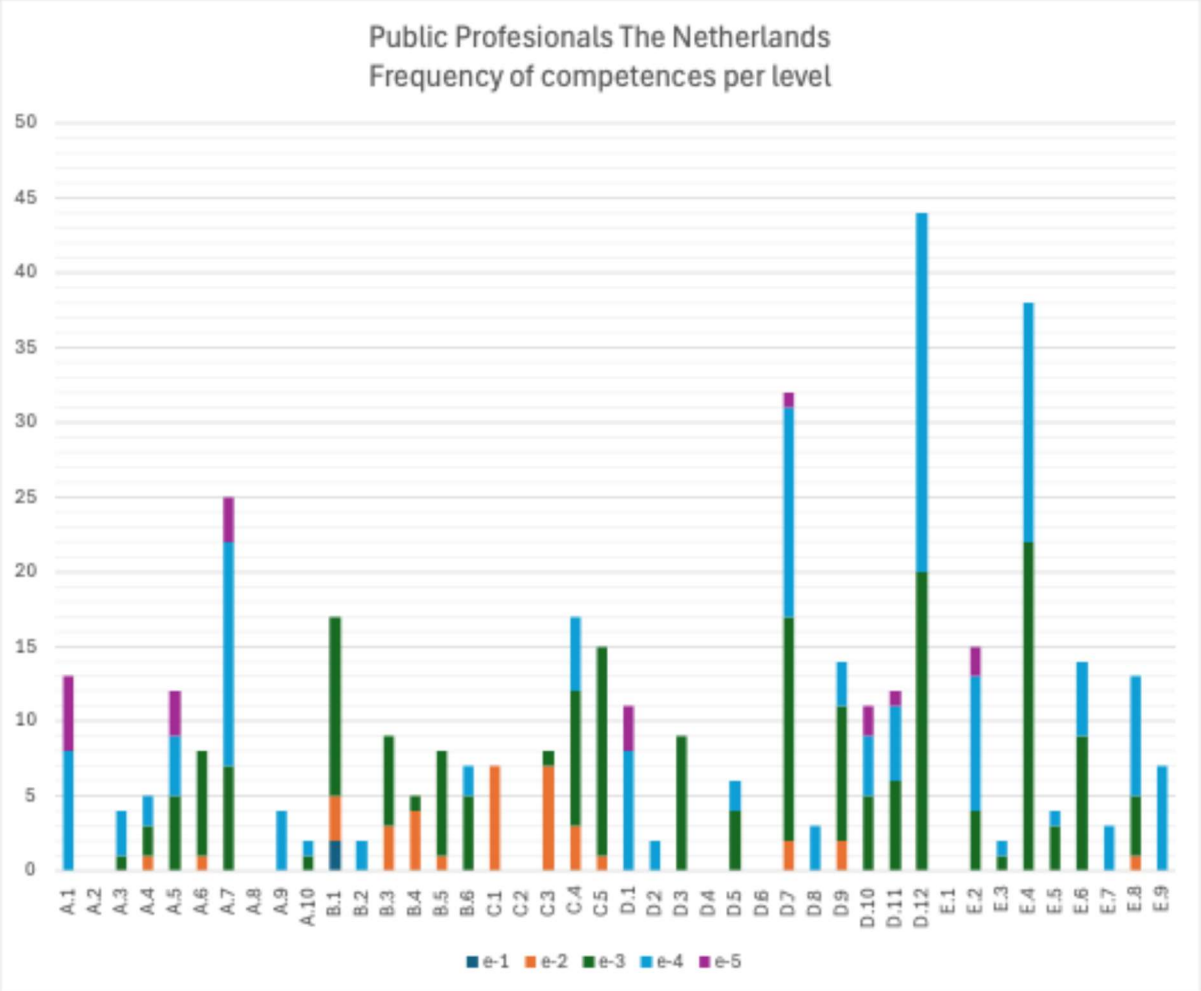

Figure 3. Required competences of public professionals in the Netherlands (n=148).

ECSF roles

The most in-demand ECSF roles from the Dutch labour market needs analysis are 'Cyber Threat Intelligence Specialist' (6,46%), 'Cybersecurity Implementer' (4,97%), 'Cybersecurity Educator' (4,76%), 'Cybersecurity Architect (4,31%) and 'Cyber, Legal, Policy & Compliance Officer'

(4,14%) (see Table 7). The Cyber Threat Intelligence Specialist role highlights the need for clarification and interpretation of a wide array of cybersecurity threats. The competences D.7. and E.4. are, amongst others, included in this ECSF role, which is a partial explanation for the relatively high matching percentage. Cybersecurity Architect and Cybersecurity Implementer are inherently coupled to each other as an architect orchestrates procedures, settings, software and systems, after which an implementer makes sure that each application, system or piece of software is properly set, build and implemented within an organisation. Both SMEs and Public Professionals require architects and implementers, either as part of their business model or as a vital component of the organisation's cybersecurity- and ICT infrastructure.

Another specific role need is highlighted through the 'Cybersecurity Educator'. Whilst logically linked competences, such as 'D.3. Education and Training Provision' (7,66%) and 'D.9. Personnel Development' (6,83%), do not have as high of a percentual match within the vacancies (see Table 7), the percentual match with Cybersecurity Educator does call for an increase in individuals that provide cybersecurity trainings and courses to stakeholders. Educational trainings and courses can either be given to educate the internal personnel of an organisation or to educate external parties.

As mentioned, governmental institutions play a central role in shaping cybersecurity frameworks through data analysis (D.7.), identification of long-term (cybersecurity) trends (A.7.), and the translation of obtained insights into comprehensive policy documents. This requires a long-term vision and a structured approach to cybersecurity management and public interest which is reflected in the collected vacancies and classified competences. As a result of a concentrated focus on planning and policy, it is logical that there is a relatively high match with the 'Cyber, Legal Policy & Compliance Officer' role.

3.1.2 Greece

The starting point of the labour-market analysis of Greece is the national scraping dataset of vacancies within the (cyber)security domain. To align with the scope of Deliverable 2.1, only vacancies that incorporate a cybersecurity component are included. The dataset is diverse, drawing from SMEs, large corporate businesses and (to a much lesser extent in publicly advertised form) governmental and knowledge institutions, and covers calendar year 2024. A total of 248 cybersecurity-related vacancies (Greece) were collected and classified in accordance with the common methodology. Within the working matrices, 247 Greek postings carry complete, linkable metadata and were used for the statistics below. The classification process has resulted in 1,371 competences being extracted from the Greek vacancies, which amounts to an average of approximately 5.6 competences per vacancy.

Vacancy dataset

The Greek vacancies are concentrated in 2024 and are **full-time (100%)**. The labour market shows high qualification and competency expectations of its workforce: the majority of job postings request **Medior (69%)** and **Senior (27%)** candidates. This is reflected in the demand for proficiency levels 3 (876 "hits") and 4 (641 "hits"), with levels 1 and 2 appearing rarely to not at

all (0 and 48 “hits”, respectively) and level 5 used selectively (56 “hits”). The strong representation of proficiency levels 3–4 can be attributed to the high share of postings from specialist suppliers (SMEs) and large corporate businesses, both of which recruit practitioners expected to enable and deliver security outcomes with limited oversight.

In terms of e-CF domains, the dataset emphasises Enable (D, 33.9%) and Build (B, 33.6%), followed by Plan (A, 19.1%) and Manage (E, 11.3%), with Run (C, 2.1%) much less represented. Using organization names, postings split into SME/other businesses ~72% (178/247) and large corporates ~28% (69/247). Almost no postings are explicitly labelled as public-sector roles in the scraping sample; public demand is therefore likely under-represented in scraped job boards.

Total Vacancies

The top five most frequently required competences in Greek vacancies are ‘D.12 Security Consulting’ (100.0%), ‘B.3 Testing’ (72.1%), ‘A.5 Architecture Design’ (47.8%), ‘A.6 Application Design’ (47.8%) and ‘B.6 ICT Systems Engineering’ / ‘B.1 Application/Product Development’ (both 47.8%). Several factors explain these high frequencies:

- **D.12 Security Consulting.** Organisations in Greece commonly seek (external) expert knowledge or expect hires to provide enablement for compliance-driven and modernisation work (e.g., NIS2/DORA read-across to practical implementations). Consulting competence is therefore baseline across many roles.
- **B.3 Testing.** With acute skills shortages and the need to industrialise assurance, employers prioritise secure SDLC and verification activities to scale protection across heterogeneous estates.
- **A.5/A.6/B.1/B.6.** Rapid digitalisation and platform uplift lead to high demand for design & build competences. Employers invest in application security, systems engineering and product development to embed security by design.
- **E.3/E.8.** Risk and ISMS management are strongly present—especially in regulated sectors—though less frequent than the hands-on design/build asks.

The near-ubiquitous presence of D.12 reflects the advisory and implementation support character of much of the Greek market in 2024. Organisations preparing for NIS2/DORA/sectoral expectations, or modernising legacy environments, frequently staff roles with explicit consulting/enablement duties, both in suppliers (SMEs/consultancies) and in technology/digital units of large corporates. This is complemented by the E.3 Risk Management (22.3%) and E.8 Information Security Management (21.5%) that show strong, presence—commensurate with ongoing ISMS/GRC initiatives to industrialise processes. These postings are often covered by the same consulting expert in Greek companies.

High, balanced demand appears for secure SDLC / application & systems build (architecture, design, development, systems engineering) and assurance (testing) indicates that productisation and platform modernisation (cloud/microservices/data platforms) are major hiring drivers, with security engineering embedded in delivery.

Concerning proficiency levels demanded (e-CF), across all competence requests recorded in Greek vacancies (n=1,621 level-specific "hits"), the distribution skews clearly to mid/high proficiency, with Level 3: 54.0% (876) and Level 4: 39.5% (641) accounting for the majority of vacancy levels needed. This profile confirms that employers in Greece predominantly target independent practitioners and specialists rather than entry-level staff.

SMEs

Of the 247 classified vacancies, **178** are from Greek **SMEs/other businesses**. The most in-demand competences from SME vacancies are 'D.12 Security Consulting' (100.0%), 'B.3 Testing' (72.3%), 'A.5 Architecture Design' / 'A.6 Application Design' / 'B.6 ICT Systems Engineering' / 'B.1 Application/Product Development' (51.3%), 'B.5 Documentation Production' (22.5%) and 'E.8 Information Security Management' (18.8%). SMEs typically provide specialised cybersecurity expertise to clients and operate/extend their solutions over time; accordingly, they exhibit stronger capabilities in Build (B) and Enable (D) type competences.

Large Corporates

Large organisations in Greece emphasise product/platform security and assurance, complemented by risk/governance capabilities to align with regulated-sector obligations (finance, telco, energy). The split still tilts to Enable + Build competences along with relevant implementation roles.

Public Professionals

Public-sector postings are **under-represented** in publicly scraped boards, inhibiting a robust sub-cut. Where observed, profiles skew towards planning, enablement, and governance (A/D/E) with selective in-house build competencies.

ECSF Roles

The most in-demand ECSF roles from the Greek labour-market analysis (≥50% role match) are 'Cybersecurity Architect' (47.8%), 'Cybersecurity Implementer' (47.8%), 'Digital Forensics Investigator' (24.7%), 'Penetration Tester' (13.0%) and 'Cyber Incident Responder' (12.2%) *(≈ tied with 'Cybersecurity Auditor' at 12.2%)*.

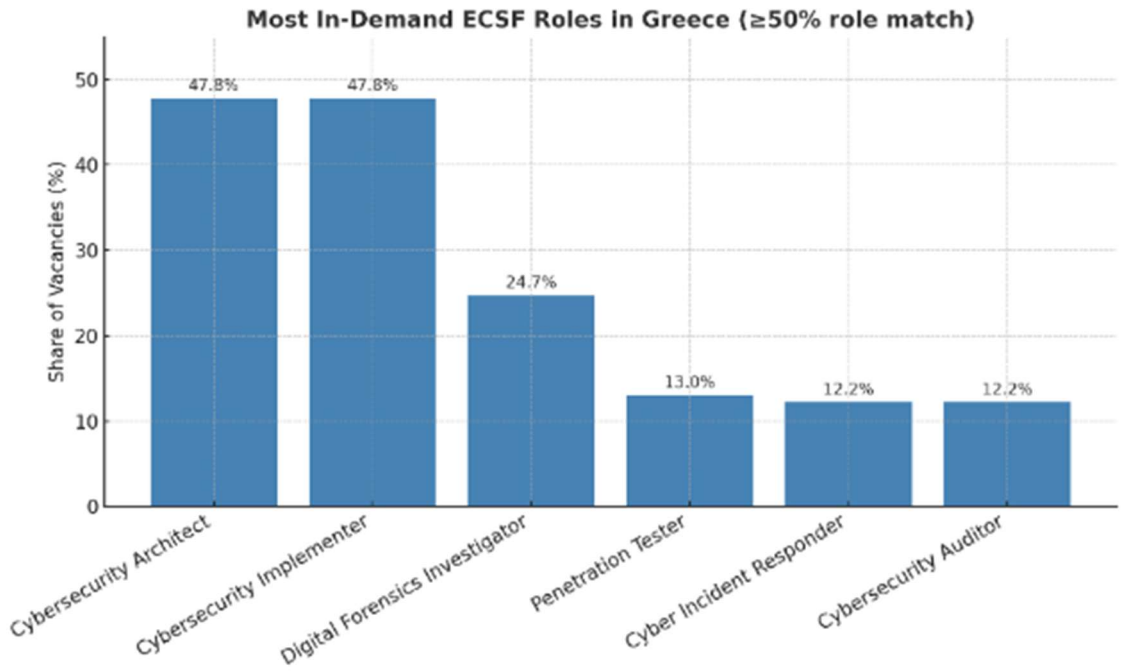

Figure 4. Most in-Demand ECSF Roles in Greek vacancies.

Architect and Implementer are inherently coupled, as the architect designs and orchestrates controls while the implementer ensures correct build and deployment. Demand for DFIR and testing reflects the need for assurance capacity and incident-facing capability alongside build programmes. Governance and policy roles are consistently present but appear less frequently in public adverts, likely due to smaller absolute numbers and internal pathways.

Insights in the labour market demand based on the job vacancy analysis

The ICT Service Management sector is experiencing increasing demand across all ECSF role profiles. The Digital Infrastructure sector sees a spike in demand for Cybersecurity Implementers (48,71%) and Penetration Testers (14,84%). Research and Academia demand more Cybersecurity Researchers (1,86%) and Cybersecurity Auditors (15,32%) (see Annex 6 Tables, figures & data Table 9).

In addition to these, several emerging or complementary roles were also identified across all sectors, including:

- Cybersecurity Liaisons
- AI Security Specialists
- Identity & Access Administrators
- Cloud Security Administrators
- SOC Analysts (closely aligned with Cyber Incident Responders
- Cybersecurity Presales Engineers

These profiles should be taken into account when developing Task T2.6 – Planning of Training Activities and Alignment with the Academy.

From a skills perspective, the most needed skills include:

- Data Analysis
- Data Privacy
- Incident Management
- Cloud Security
- Information Systems & Network Security / Cyber Resilience
- Access Controls / Identity Management
- Threat Analysis
- Communication Skills
- Problem Solving.

3.1.3 Cyprus

Vacancy dataset

The cybersecurity-related job vacancies analysed in this report were identified through systematic searches on job vacancy databases, with a primary focus on LinkedIn. The selection process involved filtering listings that explicitly referenced cybersecurity roles, competences, or responsibilities, ensuring relevance to the digital security domain. This approach allowed for the collection of a representative sample of current labour market demands in Cyprus. The total number of vacancies that have been included in 2025 is 41 (see Table 10). Although the initial aim was to gather data spanning both 2024 and 2025, relevant and complete postings were only available for the year 2025. As a result, the analysis reflects the demand for cybersecurity competences based on job listings published from 2025 onwards.

General findings

In Cyprus, the cybersecurity labour market continues to evolve, with 41 job vacancies identified for 2025. These vacancies span both the public and private sectors, with a concentration in SMEs and public institutions. Most roles require competences at proficiency levels e-2 and e-3, indicating a strong demand for professionals with solid operational (technical) expertise and the ability to work independently to a certain degree. Senior-level roles (e-4 and e-5) remain less common, reflecting the national cybersecurity ecosystem's relatively small scale and developing maturity.

The findings from the 2024 national surveys conducted by DSA reinforce this picture. Nearly half of all businesses (47%) reported experiencing at least one cyberattack in the past year, with phishing being the most common form of attack. Despite a slight decrease in attack frequency compared to previous years, the economic impact remains significant, with over half of affected businesses reporting financial losses averaging €12,000.

Interestingly, lack of awareness and training gaps persist. Half of the businesses surveyed were unaware of available cybersecurity training opportunities, and only 13% participated in such programmes. However, those who engaged in training were more likely to implement improved security measures, highlighting the importance of capacity building in the workforce.
Among citizens, 49% reported being victims of cyberattacks in the past year, with phishing again being the most prevalent threat. While the average number of attacks per person increased, the average financial loss decreased, possibly due to improved awareness and digital hygiene

practices. This suggests a growing resilience among the population, though significant gaps in training and preparedness remain.

Total vacancies

The general analysis of the 41 vacancies reveals a shift in the most frequently required competences across the national labour market of Cyprus. The top five competences are 'A.7. Technology Trend Monitoring' (56,10%), 'C.4. Problem Management' (51,22%), 'B.5. Documentation Production' (43,90%), 'D.7. Science and Analysis' (36,59%) and 'D.12. Security Consulting' (36,59%) (see Table 11).

These competences reflect a growing emphasis on strategic foresight, operational resilience, and structured knowledge management. The prominence of Technology Trend Monitoring suggests that employers are increasingly prioritising the ability to anticipate and adapt to emerging digital threats. This is particularly relevant in a region where digital transformation is accelerating across sectors such as finance, tourism, and public administration. Meanwhile, the high demand for Problem Management and Documentation Production indicates a continued focus on maintaining system integrity and ensuring clear, compliant communication. The inclusion of Science and Analysis and Security Consulting in the top five highlights a rising need for analytical and advisory roles, particularly in environments where evidence-based decision-making and expert guidance are essential.

SMEs

Among the 29 vacancies of SMEs (see Table 12), the demand remains centred on practical, implementation-focused competences. The top five competences in this segment are 'B.3. Testing' (48,28%), 'A.5. Architecture Design' (37,93%), 'A.7. Technology Trend Monitoring' (34,48%), 'C.4. Problem Management' (31,03%) and 'E.3. Risk Management' (31,03%) (see Table 13).

These findings suggest that SMEs in Cyprus prioritise professionals who can build, test, and maintain secure systems, often within lean teams. The emphasis on Testing and Architecture Design reflects the need for robust system development and deployment capabilities. Risk Management and Problem Management further underscore the importance of operational continuity and incident response in resource-constrained environments. Technology Trend Monitoring highlights the need for up-to-date knowledge on technological trends and subjects.

Public professionals

In the public sector, the demand profile is distinct, with a strong focus on strategic, analytical, and advisory competences. From the 12 vacancies (see Table 14), the most frequently required competences among public professionals are: 'A.7. Technology Trend Monitoring', 'B.4. Solution Deployment', 'B.5. Documentation Production', 'C.4. Problem Management', 'D.1. Information Security Strategy Development', 'D.3. Education and Training Provision', 'D.7. Science and Analysis' and 'D.12. Security Consulting' (see Table 15).

All these competences appear in 100% of the public sector vacancies analysed, indicating a highly consistent demand profile. Public institutions in Cyprus are clearly prioritising roles that

support strategic planning, policy development, and internal capacity building. The emphasis on Education and Training Provision and Security Consulting reflects a broader mission to enhance national cybersecurity readiness and resilience.

ECSF roles

The analysis of the Cyprus job vacancies through the lens of the ECSF highlights a strong alignment with roles centred on digital investigation, incident response, and implementation (see Table 16). The most prominent role is the Digital Forensics Investigator (13,41%), which consistently ranks highest in match percentage and frequency, indicating a significant demand for investigative and evidence-handling expertise. Additionally, the Cyber Incident Responder (9,76%) and Cybersecurity Implementer (4,39%) roles show substantial relevance, reflecting the labour market's emphasis on operational readiness and technical execution. The presence of Cyber Legal, Policy & Compliance Officers (4,27%) and Cybersecurity Educators (3,25%) further suggests a growing need for regulatory awareness and capacity-building within the cybersecurity ecosystem.

3.1.4 Croatia

General findings

During the examined period (2024–2025), the Croatian cybersecurity labour market exhibited a targeted albeit limited demand, with 82 openings documented across governmental, corporate, and small to medium-sized enterprises (see Table 18). The Croatian market, however smaller than other EU markets, exhibits a consistent framework for necessary competences and job role requirements, adhering to the e-CF. Most job postings require applicants with a competence level of e-3, followed by e-4, indicating a distinct preference for experts capable of independent operation with specialised knowledge. Positions necessitating e-4 proficiency are generally associated with strategic and leadership roles, such as senior consultants and security officers. The Croatian market prominently prioritises operational and implementation-focused roles, with Build (B) and Run (C) competences typically observed. Nonetheless, planning (A) and enabling (D) domain competences are becoming increasingly prevalent, particularly in government-related positions.

Total Vacancies

The examination of job openings in Croatia indicates that the most commonly sought competences are concentrated in 'B.5. Documentation Production (60,98%), 'C.4. Problem Management' (45,12%), 'E.3. Risk Management (41,46%), Information Security (D.1., E.8.; 40,24%, 39,02%) and 'D.12. Security Consulting' (36,59%) (see Table 18). This pattern suggests that businesses place a high priority on experts who can effectively execute cybersecurity measures, document them accurately, and contribute to strategic planning and risk mitigation initiatives. The prevalence of skills such as documentation creation, risk management, and problem management indicates the operational maturity of cybersecurity positions in the Croatian labour market, where compliance, system stability, and structured processes are fundamental to organisational resilience. The prevalence of consulting and security management positions signifies an increasing reliance on advisory expertise and systematic frameworks to guide digital security activities.

SMEs

The examination of 30 job openings from small and medium-sized firms (see Table 19) indicates a significant demand for skills in documentation ('B.5. Documentation Production', 58,62%), operational troubleshooting ('C.4. Problem Management', 48, 28%; 'C.1. User Support', 34,48%), system administration ('C.5. Systems Management', 41,38%), information security ('D.1. Information Security Strategy Development', 41,38%), and external consultancy ('D.12. Security Consulting', 37,93%) (see Table 20). These organisations generally operate with streamlined teams and require individuals to possess a diverse range of practical and readily usable skills. The significance of Build and Run competences suggests that SMEs emphasise operational efficiency and client service. The recurrent presence of consulting, information security and risk-related competences suggests that SMEs rely on adaptable expert advice to tailor security solutions to various customer contexts. Cybersecurity positions in SMEs are characterised by a pragmatic, implementation-oriented approach that prioritises multifunctionality and agility.

Public professionals

The 9 analysed cybersecurity positions in the public sector (see Table 21) are distinctly focused on risk management ('E.3. Risk Management', 88,89%), governance ('B.5. Documentation Production', 77,78%; 'E.2. Project and Portfolio Management', 66,67%; 'D.4. Purchasing,' 44,44%), strategic supervision ('E.8. Information Security Management', 66,67%; 'D.1. Information Security Strategy Development', 55,55%), and instructional responsibilities ('D.3. Education and Training Provision', 44,44%) (see Table 22). The most demanded competences illustrate the public sector's emphasis on strategic planning, adherence to regulatory standards, and enhancement of internal capacities. Government organisations seek experts who can provide policy guidance, manage risk, oversee extensive projects, and facilitate the effective dissemination of institutional knowledge, rather than those focused solely on hands-on technical implementation. That highlights the sector's significant contribution to the development of national cybersecurity frameworks and the improvement of systemic resilience through organised, policy-oriented strategies.

ECSF roles

Analysing Croatian job postings in relation to the ECSF reveals a significant correlation with positions focused on compliance, education, investigation, and strategic cybersecurity tasks (see Table 23). The predominant roles encompass Cyber legal, policy, and compliance officers (19,27%), Cybersecurity educators (14,23%), and Digital forensics investigators (10,67%), signifying that the labour market prioritises not only technological implementation but also regulatory, analytical, and educational competences.

Conclusion

The Croatian cybersecurity labour market exhibits a structured and developing demand for competences that integrate operational execution with strategic control. Organisations, both public and private, are increasingly cognisant of the necessity for specialists who not only oversee technical systems but also enhance comprehensive risk governance, compliance, and security strategies. SMEs prioritise adaptability and practical proficiency, whereas public institutions concentrate on policy formulation, education, and strategic coherence. Documentation, risk management, and advising competences are esteemed across all sectors.

3.2 Additional countries analyses: CyberHubs

One of the most prominent EU-projects in the realm of cybersecurity is CyberSecPro, and its specialisation project CyberHubs. The goal of CyberHubs is to identify key requirements for cybersecurity skills and professional roles in seven different countries, thereby considering the current state of each coutry's cybersecurity ecosystem, along with its unique opportunities and challenges (CyberSecPro, 2024). The countries involved within the project are **Lithuania**, **Spain**, **Estonia**, **Slovenia**, **Greece**, **Hungary** and **Belgium**. The following two areas, namely '*skills*' and '*roles*' (see Table 24 & Table 25) highlight the most critical cybersecurity needs. Addressing the identified gaps from each country will help strengthen cybersecurity resilience through targeted training and development.

The most trending skills across the analysed countries highlight emerging priorities within the cybersecurity domain. It is evident that data privacy (E.6.), cloud security (B.6., C.5., E.8.), network security / cyber resilience (B.6., C.4., C.5.), incident management (C.4., E.3.) and access control / identity management (C.5, E.9.) are the most mentioned skills in the country reports (see Table 24). The essence lies on the e-CF domains of Build (B) and Run (C), highlighting the need for technical skills, such as 'C.5. Systems Management' and 'C.4. Problem Management'. Competences from the Manage (E) domain, such as 'E.3. Risk Management' and 'E.6. Quality Management and Compliance' also come to forth, pressing the need for incident- and risk management and data privacy control mechanisms. Besides, there is a general need for 'soft skills', such as communication skills, team-building skills and leadership skills. Soft skills are not directly linked to the e-CF but are worth to be mentioned.

Furthermore, each country has identified a lack of Cyber Incident Responders (7x) and Cybersecurity Implementers (7x) (see Table 25). This is logical, as the skills gaps have shown that competences such as B.6. and C.4. are in high demand. The role demand provides, besides Build (B) and Run (C) competences, further insights in skills demand, namely in the realm of Plan (A). Architecture Design (A.5.) and Application & Product Design (A.6.) are essential competences for a Cybersecurity Implementer. The role of Cybersecurity Architect (5x) reaffirms the domain emphasis on Plan (A), Build (B) and Run (C), as A.5., A.6., B.1., B.3. and B.6. are embedded within this role. These roles are all-in-all fairly technical and sophisticated in nature, highlighting the proper need for hard technical skills within Lithuania, Spain, Estonia, Slovenia, Greece, Hungary and Belgium. Contrary to these three roles, but in line with the mentioned skill demand, is the CISO role (5x). This role is mainly focused on the domain Manage (E), shown through the competences E.3., E.8. and E.9.. The identified skill E.3. can directly be linked to the CISO demand, and shows that besides technical roles, management roles are in demand as well.

3.3 Summarisation labour market needs

The most frequently addressed competences for The Netherlands, Cyprus and Croatia are the following: 'E.8. Information Security Management' (21,45%), 'E.3. Risk Management' (17,82%), 'C.4. Problem Management' (16,17%), 'B.5. Documentation Production' (14,96%) and 'B.3. Testing' (12,21%) (see Table 65 and Figure 5). On the one hand, the focus lies on abilities to test system operability, solve system malfunctions and properly document each step of the process. On the other hand, there is a need for regulation, policy and oversight in the realms of information security and risk management.

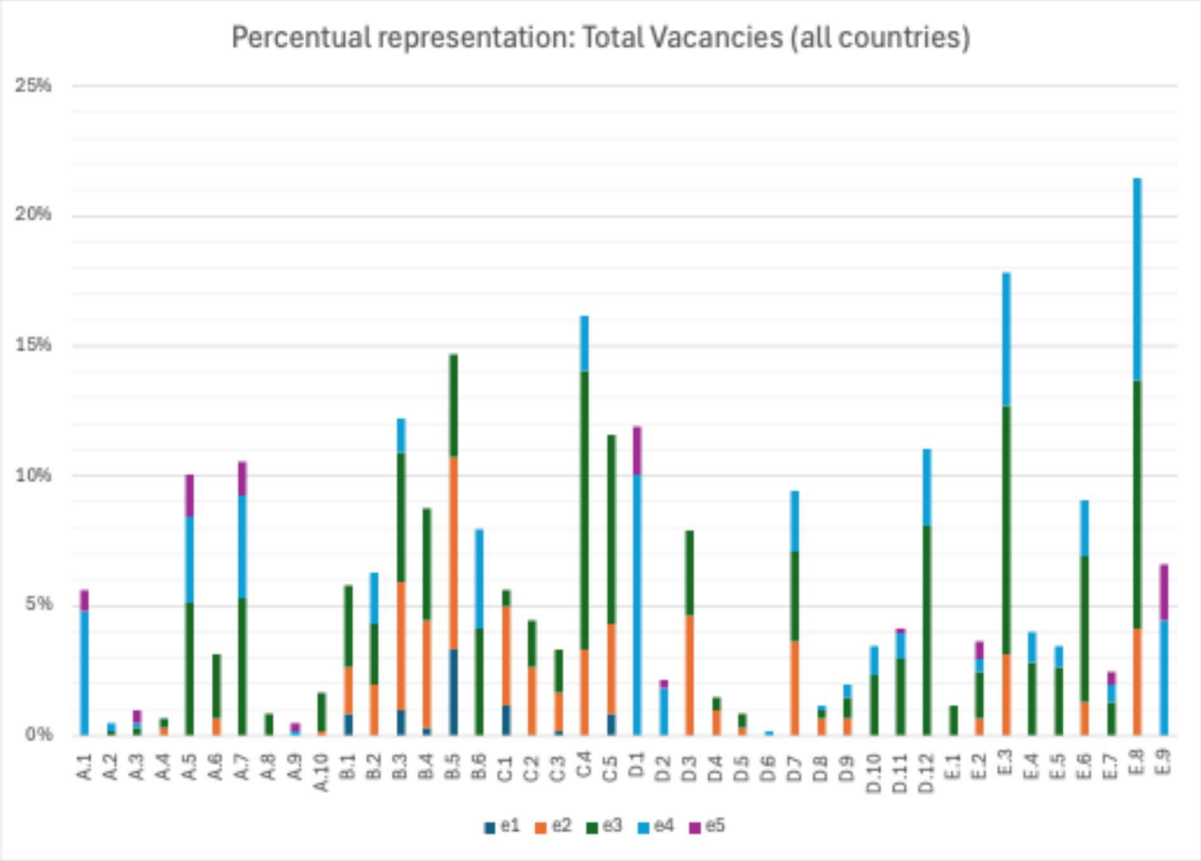

Figure 5. Most frequently required competences for the Netherlands, Cyprus and Croatia.

Regarding SMEs it is shown that 'D.12. Security Consulting' (9,74%), 'C.4. Problem Management' (6,77%), 'C.5. Systems Management' (5,78%), 'B.5. Documentation Production' (5,45%) and 'B.1. Application/Product Development' (4,62%) (see Table 65) form the top five competences for The Netherlands, Cyprus and Croatia. SMEs have a heightened focus on creating or developing products or applications for internal or external stakeholders, which is why competences such as problem solving, system managing and documentation are essential for the day-to-day operations of SMEs. Consequently, once an application or product is developed, consultation abilities are essential to propagate their product.

The top five competences for Public Professionals are 'D.12. Security Consulting' (9,74%), 'D.7. Science and Analysis' (7,26%), 'E.4. Relationship Management' (6,44%), 'A.7. Technology Trend Monitoring' (6,27%) and 'C.4. Problem Management' (4,95%) (see Table 65). As governmental institutions are generally focused on writing and developing policies for a wide variety of topics, analytical and trend monitoring abilities are essential to possess. Furthermore, additionally to in-house knowledge and talent, governmental institutions tend to inform external consultants for their expertise. Therefore, there is an increased need for security consulting and relationship management in this domain.

As shown in Table 66 the overlapping ECSF roles for the Netherlands, Cyprus and Croatia are Cyber, Legal, Policy & Compliance Officer (7,80%), Cybersecurity Educator (6,33%), Cybersecurity Researcher (4,72%), Digital Forensics Investigator (4,45%) and Cyber Threat Intelligence Specialist (4,19%). The need for regulatory oversight within the public domain explains the match with Cyber, Legal, Policy & Compliance Officer. Competences such as 'D.7. Science and Analysis' and 'A.7. Technology Trend Monitoring' provide an explanation for the overlap with Cybersecurity Researcher and Digital Forensics Investigator. Cybersecurity Educator and Cyber Threat Intelligence Specialist have their overlapping merit in 'E.8. Information Security Management'.

The competences distilled from the CyberHubs analysis are combined with the vacancy analysis results i to strengthen the gap analysis. Each identified competence provides insights into the needs of seven additional countries. What can be seen in Table AA is that 'C.5. Systems Management' (12x), 'B.6. ICT Systems Engineering' (11x), 'C.4. Problem Management' (9x), 'E.3. Risk Management' (5x), 'E.6. Quality Management & Compliance' (5x) and 'E.8. Information Security Management' (5x) are reinforced through the CyberHubs analysis. The vacancy analysis and CyberHubs analysis, in conjunction with competences distilled from the literature review, trend analysis and focus groups establish the overall labour market demand of the Netherlands, Cyprus and Croatia in the gap analysis. The vacancy analysis is the most extensive part of the overall labour market demand, as the analysis is based upon the collection and labelling of competences from hundreds of vacancies. The CyberHubs analysis is based upon seven country reports, from which skills are distilled and consequently linked to e-CF competences. Overall, this means that less competences are collected from the CyberHubs analysis. However, the CyberHubs analysis in conjunction with the literature review, trends analysis and focus groups provide comprehensive insights into the overall labour market demand.

	Total frequency vacancy competences per level					**CyberHubs competences required**						
Competence/ Proficiency level	**e1**	**e2**	**e3**	**e4**	**e5**	**Lithuania**	**Spain**	**Estonia**	**Slovenia**	**Greece**	**Hungary**	**Belgium**
A.1. IS and Business Strategy Alignment	0	0	0	29	5							
A.2. Service Level Management	0	0	1	2	0							
A.3. Business Plan Development	0	0	2	1	3							
A.4. Product/ Service Planning	0	2	2	0	0							
A.5. Architecture Design	0	0	31	20	10					1		
A.6. Application/ Product Design	0	4	15	0	0							
A.7. Technology Trend Monitoring	0	0	32	24	8							
A.8. Sustainability Management	0	0	5	0	0							
A.9. Innovating	0	0	0	1	2							

A.10. User Experience	0	1	9	0	0								
B.1. Application/ Product Development	5	11	19	0	0								
B.2. Component Integration	0	12	14	12	0			1	1				
B.3. Testing	6	30	30	8	0						2		
B.4. Solution Deployment	2	25	26	0	0								
B.5. Documentation Production	20	45	24	0	0			1	1				
B.6. ICT Systems Engineering	0	0	25	23	0		1	3	2	1	2	1	1
C.1. User Support	7	23	4	0	0								
C.2. Change Support	0	16	11	0	0								
C.3. Service Delivery	1	9	10	0	0								
C.4. Problem Management	0	20	65	13	0		1	3	2	1	2		
C.5. Systems Management	5	21	44	0	0		2	2	2	1	2	1	2
D.1. Information Security Strategy Development	0	0	0	61	11								
D.2. Quality Strategy Development	0	0	0	11	2								
D.3. Education and Training Provision	0	28	20	0	0								
D.4. Purchasing	0	6	3	0	0								
D.5. Sales Development	0	2	3	0	0								
D.6. Digital Marketing	0	0	0	1	0								
D.7. Science and Analysis	0	22	21	14	0				1				
D.8. Contract Management	0	4	2	1	0								
D.9. Personnel Development	0	4	5	3	0								
D.10. Information and Knowledge Management	0	0	14	7	0								
D.11. Needs Identification	0	0	18	6	1								
D.12. Security Consulting	0	0	49	18	0								
E.1. Forecast Development	0	0	7	0	0								
E.2. Project and Portfolio Management	0	4	11	3	4								
E.3. Risk Management	0	19	58	31	0			2	2		1		
E.4. Relationship Management	0	0	17	7	0								
E.5. Process Improvement	0	0	16	5	0								
E.6. Quality Management and Compliance	0	8	34	13	0		1	1	1		1	1	
E.7. Business Change Management	0	0	8	4	3								
E.8. Information Security Management	0	25	58	47	0			1	1		1	1	1
E.9. Information Systems Governance	0	0	0	27	13		1		1				1

Table AA. The Netherlands, Cyprus, Croatia – Total frequency of vacancy competences matched with CyberHubs competences

3.4 Adjustments to and creation of ECSF roles

Firstly, it can be said that the 12 ECSF roles are based on a logical and factually supportable foundation of competences. However, the specific competency levels appear to require further adjustments, which is to be expected when comparing these roles to continuously developing labour markets. It is to be noted, that the dataset used for this analysis is just over 600 vacancies, which is a minimal amount of data to conduct the evaluation of the ECSF roles. Secondly, the discrepancies in competence assignment to each vacancy hinder the immediate evaluation of the data and the formulation of the analysis noticeably. It is very visible that the value of the match-based analysis was greatly diminished by these inconsistencies. It is highly recommended to develop a protocol dictating how to evaluate vacancies, especially in regard to the number of assigned competences used per vacancy. Based on the findings in this analysis, this report suggests the minimum usage of 4 and maximum of 6 competences per vacancy. With that, the vacancies can theoretically have a better matching with the ECSF roles, as theirs range between 3 competences (applicable to one ECSF role) and 5 competences (applicable to 10 ECSF roles). This will allow the evaluator of the vacancy to tag the fundamental tasks of the vacancy, including the most important contextually implied task(s).

Despite of these limitations, the data does support the recommendations for the development of 3 forward looking ECSF roles (*Security Governance Manager, Compliance Officer, Threat Innovation Analyst*) and recommends valid adaptions of various degrees to the existing ECSF roles (see Table AB). To read the full analysis and for further development, as well as argumentation for the given recommendations, please refer to Annex 8.

ECSF Role	Recommended changes	New role suggestions
Chief Information Security Officer (CISO)	Change: E8 (e3) to E8 (e4) Add: A1(e5)	Security Governance Manager
Cyber Incident Responder	Change: C4 (e4) to C4 (e3) Add: D1(e4)	
Cyber Legal, Policy & Compliance Officer	None, the competences seem well placed in relation to labour market demand	Compliance Officer
Cyber Threat Intelligence Specialist	None, the competences seem well placed in relation to labour market demand	Threat Innovation Analyst
Cybersecurity Architect	Add: E4 (e4) Remove: B3	
Cybersecurity Auditor	Remove: B3 Change: E3 (e4) to E3 (e3) Add: E4 (e3)	
Cybersecurity Educator	Redefine or remove D9 Add: B1(e3)	
Cybersecurity Implementer	Add: C5 (e3)	
Cybersecurity Researcher	Remove: C4 Add: E4 (e4) Add: D9 (e3) Change: A7 (e5) to A7 (e4) Change: A9 (e5) to A7 (e4)	
Cybersecurity Risk Manager	Add: B5 (e2)	
Digital Forensics Investigator	Change: B3 (e4) to B3 (e3) Add: D7 (e3)	
Penetration Tester	None, the competences seem well placed in relation to labour market demand	

Table AB. Potential new ECSF roles and proposed adjustments to current roles based on needs analysis.

4 EXPECTED FUTURE NEEDS

4.1 Literature review EU projects on labour & education market

Europe faces several shortages within the cybersecurity labour market, both in terms of number of people and in their competences, such as the required cybersecurity-, soft- and hard skills amongst professionals and teachers (see Table 26) (REWIRE, 2023, p.20). The European Union has funded several initiatives that focus on cybersecurity in relation to the European labour market, namely CONCORDIA, CyberSec4Europe, CyberSecPro, ECHO, NERO, REWIRE and SPARTA. ENISA also plays a vital role in the cybersecurity labour market. In particular, ENISA has developed the ECSF in which 12 cybersecurity job profiles are developed, each with their own corresponding tasks, knowledge areas, skills and (e-CF) competences (CyberSecPro, 2022a, p.1). Each EU-project aims to harness knowledge from the corresponding projects' results to avoid duplicate work and a 'reinvention of the wheel' (CyberSecPro, 2022a, p. 4-5). On the one hand, CONCORDIA and CyberSec4Europe focus on boosting cybersecurity competences and facilitating cybersecurity trainings through cyber ranges across Europe (CyberSecPro, 2022a, p.1). On the other hand, CyberSecPro, ECHO, REWIRE and SPARTA have developed cybersecurity workforce skills frameworks and cybersecurity curricula to support European training providers with the development of cybersecurity trainings and courses (CyberSecPro, 2022a, p.1; ECHO, 2021). However, despite the efforts of each EU-project, the cybersecurity skills gap in the EU is increasing (Polemi & Kioskli, 2023, p.94). In particular, a cybersecurity skills gap is visible between curricula of educational institutions and market demand (see Table 27).

There is a wide variety of key issues affecting cybersecurity education that are mentioned in the multitude of EU projects, visualised in Table 26. The most pressing issue in today's cybersecurity labour market landscape is that there is a lack of cooperation and poor interaction with and within the cybersecurity industry. This means that stakeholders are either unwilling to cooperate with other stakeholders, are not aligned in terms of cybersecurity goals or do not encompass the required skills or competences to align individual cybersecurity initiatives. As shown by the mentioned EU-projects, there are indeed a multitude of cooperative efforts, both on a national and European scale which helps the cybersecurity sector in various ways. However, these efforts are not enough to properly address the most pressing issues. To partially solve the issue, the competence 'E.4. Relationship Management' can be integrated in the development of trainings and courses.

Furthermore, the analyses of the EU-projects shows that there is a sincere lack of cybersecurity professionals (see Table 27), particularly cybersecurity educators, and a lack of training resources (see Table 26). A high demand for (and inherent lack of) cybersecurity specialists is also driven by growing national, European and international cybersecurity guidelines, such as the NIS2 and DORA (see Table 27). Through the launch of promotional campaigns, cybersecurity professionals, -educators and -specialists can be attracted to the cybersecurity domain. Consequently, it is necessary to focus on D.3. Education and Training Provision in order to properly train new personnel and improve the skills and competences of current cybersecurity educators. The matter of a lack of resources for cybersecurity education differs per country, but generally requires political interference on regional, sectoral, national and EU-level to be

properly addressed. As cybersecurity is a fast-developing domain, the most pressing issues are increasingly put on national agendas.

It has also become evident that the set of skills for cybersecurity professionals is changing due to altering cyberattacks (see Table 26). Due to geopolitical tensions, cyber threats have increasingly become more sophisticated (see Table 27) to which cybersecurity professionals need to adjust. It has become clear that cybersecurity professionals increasingly require a mix of hard and soft skills (see Table 27). The changing cybersecurity landscape also causes a lack of awareness of current cybersecurity risks (see Table 26). SMEs and public professionals need to be aware of the altering landscape in which they operate, for which it is required to constantly improve and develop skills and competences for internal personnel ('D.9. Personnel Development'). Besides, through awareness campaigns and workshops, personnel can be trained to watch out for new cybersecurity risks and threats, thereby improving the overall (information) security of the organisation.

To counter the evolving cyber threat landscape, key competence areas require greater emphasis in training development. The identified cybersecurity threats, such as ransomware, malware, social engineering and disinformation (see Table 28) have their merit in the REWIRE Project reports, ENISA Threat Landscape reports, additional trend reports and EU projects. The biggest cumulative competence needs identified to counter the current *cyberthreat* and *cyber issue* landscape are 'B.3. Testing' (6x), 'D.3. Education and Training Provision' (6x), 'D.9. Personnel Development' (6x) 'C.4. Problem Management' (4x), 'C.5. System Management' (4x), 'E.3. Risk Management' (4x) and 'E.8. Information Security Management' (4x). These competences highlight the significant need for the improvement of employees' skills through training and on the job learning, particularly in the realms of, problem solving, system management and -testing, risk management and information security management.

4.2 Trend analysis

Three categories of trends shaping the cybersecurity and digital risk landscape were identified in 20 analysed trend reports (ASD, 2024; Cisco, 2024; CrowdStrike, 2025; Deloitte, 2024; ENISA, 2023; ENISA, 2024a; ENISA, 2024b; Gallagher, Brandt & Wisniewski, 2024; Gartner, 2025; ISACA, 2024; NCSC NZ, 2024; NCTV, 2024; NOREA, 2025; NTT Security Holdings, 2024; PTvT/Dialogic, 2024; PwC, 2025a; PwC, 2025b; REWIRE, 2024; World Economic Forum, 2025):

1. regulatory tightening,
2. technical developments, and
3. security and risk changes.

Regulatory tightening is driven by a surge in EU regulations like NIS2, DORA, CRA, and the AI Act, which demand stricter compliance, cross-border oversight, and secure-by-design principles, a development approach where security is integrated from the initial design phase, rather than added as an afterthought. Organisations must now manage overlapping legal requirements, ensure operational resilience, and address artificial intelligence (AI)-related risks such as algorithmic bias and transparency. This trend emphasises the need for competences in legal-technical alignment, incident response, supplier security, and cross-functional collaboration, especially in sectors newly classified as "essential" or "important" such as digital

infrastructure, cloud providers, and public administration. Technical developments highlight the dual use of AI in both cyberattacks and defence. Threat actors are leveraging AI tools like FraudGPT and Large Language Models (LLMs) for phishing, malware, and deepfake scams, while defenders use AI for automated patching and threat detection. The rise of cloud and Software as a Service (SaaS) exploitation, attacks on open-source software, and the targeting of edge and IoT devices underscore the need for skills in secure software development, cloud security, and AI governance. Meanwhile, evolving security and risk dynamics—driven by geopolitical tensions, complex supply chains, and state-sponsored attacks—demand capabilities in global threat analysis, public-private collaboration, and resilience planning. An overview of the most dominant trends relating to regulatory tightening, technical developments and security and risk challenges and their implications for competences is provided in Table AC.

Dominant trends	**Related competences related to one or more dominant trends**
Regulatory tightening	
- Third-party risk oversight: regulations increasingly demand visibility into supply chain security. - Enhanced incident reporting, stricter supply chain oversight including SBOM requirements (WEF, Sophos). - Increased accountability for boards of directors due to the NIS2 directive. - The DORA, the EU's General Data Protection Regulation (GDPR) extend regulatory scrutiny across sectors and borders and introduce challenges, such as managing overlapping requirements, achieving compliance in multiple jurisdictions and addressing varied enforcement timelines. - Mandatory compliance with a growing body of EU regulations (e.g. NIS2, CRA, DORA, AI Act) for a wide range of sectors and services. More entities are now considered "essential" or "important" under NIS2, including digital infrastructure, cloud providers, and public administration. - The EU is pushing for Secure-by-Design principles in digital products, requiring vendors to embed security from the outset. - Regulatory focus is increasing on AI misuse, data ownership, and algorithmic bias, especially in high-risk sectors like law enforcement and healthcare. - CRA mandates secure-by-design and secure-by-default principles for digital products. - Operational resilience in the financial sector is governed by DORA, requiring ICT risk management and third-party oversight. - Increased enforcement power**:** Supervisory authorities can impose significant fines. - AI Act requires conformity assessments, transparency, and human oversight for high-risk AI systems. - Interoperability Standards: EU regulations push for standardised APIs and data formats to enable seamless data exchange.	- Skills in managing cross-border compliance programmes and audit. (E.6.) - Ability to evaluate and enforce supplier security standards. (E.6.) - Translate technical risks into business language (for non-technical stakeholders). (D.12.) - Implementing incident response protocols and ensuring the ability to continue critical operations even under degraded conditions. Specific attention is needed for securing OT environments, such as manufacturing equipment, logistics systems, and smart building infrastructure, which are increasingly exposed to cyber risks. (C.4.) - Ability to align technical operations with legal obligations, including data reuse, metadata standards, and interoperability. (D.7.) - Skills in privacy-by-design and secure data lifecycle management. (A.5.) - Continuously interpret and update regulatory interpretation (e.g. GDPR, NIS2, CRA). (E.6.) - Ensure logging, traceability, and explainability of AI systems. (D.7.) - Cross-functional collaboration with data scientists and legal teams. (E.4.) - Skills in assurance, auditing, and certification processes to ensure compliance. (E.6.)

Technical developments	
- Cybercriminals increasingly use AI tools like FraudGPT and large language models to craft scam emails, generate malicious scripts, and enhance phishing campaign. AI is also used in influence operations and deepfake scams. - Use of Living Off The Land (LOTL) and Living Off Trusted Sites (LOTS) tactics to avoid detection. - Attacks on open-source libraries and third-party software are growing, with potential for systemic impact. - Growing awareness in preparing for post-quantum cryptography. - Human Vulnerabilities: Misconfigurations, poor credential hygiene, and weak MFA implementations remain top risks; callback phishing and help desk impersonation; attackers exploit human trust and weak MFA. - LLM agents are beginning to autonomously exploit vulnerabilities (e.g., one-day and zero-day exploits). - Private companies increasingly rely on third-party cloud services, software platforms, and digital infrastructure-often provided by non-EU tech giants like Microsoft, Google, and Amazon. While these services enhance flexibility and scalability, they also introduce strategic dependencies and potential vulnerabilities. - Cloud and SaaS Exploitation: Cloud misconfigurations, SaaS abuse, and identity-based attacks (e.g., password spraying, token theft) are rising. - Defensive use of AI includes LLM-powered honeypots, automated patching, and threat detection. - Threat actors exploit legitimate cloud services (e.g., Slack, GitHub, Google Drive) for malware delivery and data exfiltration. - Edge devices, e.g., routers, Virtual Private Networks (VPNs) and IoT systems are increasingly targeted due to poor patching and misconfigurations.	- Skills in collecting, analysing and acting on (AI) threat data. (D.7.) - Rapid detection, containment, and investigation capabilities. (E.3.) - Skills related to ethical hacking and Penetration Testing, especially in OT and IoT systems. (B.3.) - Skills in securing cloud environments, managing identities, and enforcing zero-trust architectures. (C.5.) - Competences in secure software development, SBOM, and Continuous Integration/Continuous Delivery (CI/CD) pipeline security. (B.1.) - Expertise in securing embedded systems, firmware analysis, and network segmentation. (B.6.) - DevSecOps and Secure Coding: Integrating security into software development and deployment pipeline. (B.1.) - Skills in deploying and governing AI tools, including LLMs and Machine Learning (ML) Security Operations (SecOps). (D.7.) - Understanding of cloud migration, edge device hardening, and secure architecture design. (A.5.) - Skills in developing playbooks, conducting tabletop exercises, and managing ransomware/extortion scenarios. (D.3.) - Ability to design and deliver effective user education programmes to mitigate human error. (D.3.)
Security and risk changes	
- Escalating geopolitical tensions are contributing to a more uncertain environment. - Increased integration of and dependence on more complex supply chains is leading to a more unpredictable risk landscape. - The rapid adoption of emerging technologies is contributing to new vulnerabilities as cybercriminals harness them effectively to achieve greater sophistication and scale. - Urgent need for public–private cooperation to enable global regulatory harmonisation and alignment and ensure the applicability of cybersecurity standards throughout diverse regions. - State-sponsored attacks are increasing, targeting critical infrastructure like energy grids, healthcare systems, and defence networks. - Ransomware tactics now include double and triple extortion, combining data theft, encryption, and public shaming. - Specific attention is needed for securing OT environments, such as manufacturing equipment, logistics systems, and smart building infrastructure, which are increasingly exposed to cyber risks.	- Skills in analysing Tactics, Techniques, Procedures (TTPs) and linking them to an increasing and diverse array of global actors. (E.3.) - Ability to respond to global, complex, multi-vector attacks and conduct post-incident analysis. (C.4.) - Working with public-private partnerships, Information Sharing and Analysis Centres (ISACs), and Computer Emergency Response Teams (CERTs). (E.4.) - Ability to prioritise global threats and align security with business impact in an increasing insecure global environment including incident response, business continuity, and recovery strategies. (E.7.)

Table AC. Most dominant trends and implications for competences from the trend analysis

4.3 Focus groups

Three rounds of focus groups were organised: 1. Pilot focus group; 2. Focus groups with representatives of the public and private sector; and 3. Focus groups with representatives of education. The summary results per focus group are the following, details are in Annex 7 Results focus groups.

4.3.1 Pilot group

The first focus group confirmed the quality of the proposed methodology. It demonstrated that this approach to organising focus groups was effective in eliciting rich and in-depth reflections from participants on the interpretation of cybersecurity trends and competence gaps.

The first focus group resulted in an in-depth reflection of participants on four interrelated cybersecurity trends: increasing complexity of threats, the shift to cloud and hybrid infrastructures, evolving legislation, and the rise of automation and AI in security operations. Participants emphasised that complex threats are often driven by technological shifts and malicious use of AI, posing risks to privacy, critical infrastructure, and national security. The transition to cloud and hybrid systems necessitates attention raising concerns about dependency on major tech providers and the need for European alternatives. New regulations, particularly NIS2, challenge municipalities and SMEs, highlighting the importance of societal-level risk management. AI intensifies cyber threats, including deepfake fraud, underscoring the need for awareness and training. General reflections reveal disparities in cybersecurity skills across organisations, with small entities and municipalities facing resource constraints. The ambiguity of roles in cybersecurity implementation further complicates resilience efforts. Educational implications include the need for soft skills, ethical awareness, and interdisciplinary approaches.

Participants mentioned that there are three major challenges around cybersecurity:

- A lack of basic cyber security skills.
- Staff shortages on a technical and managerial level (e.g. CISO).
- Role ambiguity around the implementation of cybersecurity.

To become cyber resilient, organisations must work on: (1) prevention (emergency plans, risk management); (2) Protection (securing systems, devices and applications); (3) Promotion (promoting cybersafe behaviour) and (4) Preparation (being equipped to respond to incidents). Organisations need proper support from experts and authorities in cybersecurity. Greater responsibilities must be placed on suppliers and service providers to deliver secure systems. In education, more attention should be paid to soft skills, leadership/management skills, ethics and interdisciplinary working.

4.3.2 Public sector professionals

Participants emphasised that AI-enhanced cyber threats, such as deepfakes and synthetic voice attacks, are no longer hypothetical and pose serious risks, especially in phishing and social engineering. Participants expressed concern over growing digital dependencies on non-

EU cloud providers, which threaten digital sovereignty and complicate regulatory compliance. Cyber resilience and recovery were emphasised as essential, particularly considering recent ransomware attacks on public services, but must be supported by prevention and inter-organisational cooperation. Fragmented IT systems, under-protected critical sectors, and a lack of digital literacy among non-IT staff were identified as major vulnerabilities. Finally, a severe shortage of cybersecurity professionals—especially in leadership roles—combined with outdated frameworks and communication gaps with decision-makers, undermines the ability to respond effectively to evolving threats.

The most import implications of these trends for competences are:

- Cybersecurity professionals need new skills to spot, understand, and respond to threats that are powered by AI. They should be able to use AI tools and data to detect suspicious activity—while also knowing the risks of relying too much on these technologies.
- Cybersecurity professionals need the skills to keep cloud environments secure and manage the risks that come with using third-party providers. This includes checking if vendors meet security standards and following new regulations like NIS2 and DORA. Cybersecurity professionals need to be able to detect and respond to cyber incidents quickly and help systems recover with as little downtime as possible. This includes planning ahead to keep services running and protect critical functions in society during and after an attack.
- Cybersecurity professionals need to connect cybersecurity with the organisation's overall goals. This means helping leadership understand cyber risks, making sure security is part of decision-making. Cybersecurity professionals need the skills to build security into software from the very beginning. Security should be part of design, development, and testing, not just something added later.
- Cybersecurity leadership requires the ability to clearly communicate complex technical issues to non-technical stakeholders, including executives and external partners. It also involves taking responsibility during critical incidents and addressing the ethical implications of emerging technologies.

4.3.3 Private sector professionals

Participants experience that AI is rapidly transforming both cyber threats and defences, with participants noting its growing role in automating attacks and enhancing incident response. The shift to multi-cloud environments and third-party services has made cybersecurity governance more complex, especially for SMEs facing high compliance costs under regulations like NIS2 and DORA. Operational resilience is increasingly prioritised, but many smaller organisations lack the resources to test or maintain effective incident response capabilities. A widespread shortage of cybersecurity professionals—particularly those with AI expertise or strategic oversight—limits the sector's ability to meet regulatory demands and build long-term resilience. Participants emphasised that the most difficult challenge is aligning compliance, innovation, and resilience in the face of limited staffing and rapidly evolving threats.

The most import implications of these trends for competences are:

- Cybersecurity professionals must secure cloud environments by configuring access controls, detecting threats, ensuring compliance with standards and laws, and managing risks across multiple providers.
- Cybersecurity professionals need specialised skills to secure industrial control systems in critical sectors like energy and transport, applying tailored risk analysis and regulatory compliance (e.g., NIS2).
- Cybersecurity professionals need to have the ability to investigate cyber incidents, collect digital evidence, and use findings to strengthen future defences is essential.
- Cybersecurity must be integrated from the design phase, including secure coding practices, component selection, and protection throughout the development lifecycle.
- Cybersecurity professionals must identify and prioritise risks, align security strategies with business and legal goals, and clearly communicate these risks to leadership.
- Cybersecurity professionals should be able to explain complex issues to non-technical audiences, adapt to emerging threats, act ethically, and collaborate across disciplines.

The focus groups revealed few notable differences between countries. However, one significant exception emerged. In the private sector focus group, the same EU regulations (NIS2/DORA) were perceived quite differently. In Croatia, smaller companies responded with alarm. IT personnel hastily implemented firewalls and two-factor authentication, often without a coherent strategy, and opted to keep all operations in-house due to a pervasive lack of trust in external providers. In contrast, Greek participants emphasised regulatory compliance within complex IT infrastructures. The challenge there was less about panic and more about the structural difficulty of monitoring and adhering to regulations with insufficient skilled personnel

4.3.4 Upper secondary education

Participants emphasised that cybersecurity education for students aged 16–20 must move beyond theory and include practical, hands-on learning environments using real tools and scenarios. Currently, cybersecurity is only marginally addressed in secondary education, with inconsistent and superficial coverage. Rapid technological change outpaces curriculum updates, leaving students underprepared for real-world challenges. Early exposure through engaging activities like competitions and projects helps students discover their interest and build motivation. Game-based and challenge-driven learning, especially when collaborative, makes cybersecurity more relevant and exciting. However, structural barriers such as limited time, funding, and equipment often prevent teachers from implementing these approaches. Girls face additional challenges due to stereotypes, narrow framing of cybersecurity as purely technical, and lack of visible female role models. Broadening the subject to include ethical, communicative, and interdisciplinary aspects can make cybersecurity more accessible and appealing to a wider range of students, especially young women.

4.3.5 Higher education

Participants emphasised that higher cybersecurity education must be grounded in strong theoretical foundations—without understanding core concepts like Domain Name System (DNS) or cryptography, practical exercises risk becoming superficial. However, national qualification frameworks often change too slowly, making it difficult for curricula to keep pace

with evolving cybersecurity roles and technologies. True workplace readiness requires a balance of theoretical knowledge and hands-on skills, yet education systems often emphasise one at the expense of the other. Practice-based learning is most effective when it is social, physical, and active, taking place in dedicated spaces that mirror real-world cybersecurity environments. Students are more motivated when they have ownership over their learning, especially through flipped classrooms and peer-led projects. Controversial topics like hacker ethics and grey hat practices spark strong engagement by connecting technical content to real-world dilemmas. Yet, educators face barriers such as limited access to stable, well-equipped learning spaces, which are essential for active teaching methods. Finally, while female students don't want special treatment, they benefit from inclusive environments, visible role models, and broader representations of cybersecurity that go beyond programming to include communication, ethics, and social impact.

In the two educational focus groups, two key differences emerged between the participating countries. First, participants in the Netherlands frequently reported a strong emphasis on interdisciplinary education and socio-communicative skills, whereas in other countries, the focus appeared to be more on foundational cybersecurity knowledge. Additionally, the focus group members observed that attracting more women to the cybersecurity field is perceived as the greatest challenge in the Netherlands; in contrast, participants from other countries indicated that gender representation in their contexts seems to be more balanced.

The table below (Table AD) provides a summary of the most frequently mentioned competency content. Only the competences that were discussed in the focus groups are included.

Competence	Dominant future competences content from focus groups
A.1. IS and Business Strategy Alignment	Providing pro-active AI-enabled defence strategies; build information strategy in relation to digital sovereignty; long-term vendor lock-in; linking cybersecurity to legal, financial, and operational priorities; strategic oversight: especially with emerging technologies.
A.6. Application/ Product Design	Building systems and applications that are secure from the start: thinking about security early in the design process, choosing safe components, and making sure that every step of development includes the right protections.
A.7. Technology Trend Monitoring	The skill to interpret complex threats and stay current with fast-evolving technologies; the capacity to adjust to new technologies and threats quickly and to proactively learn emerging tools and practices.
B.1. Application/ Product Development	Protecting devices like bodycams, drones, and industrial sensors; applying secure-by-design principles within agile development teams; integrating security checks and testing into CI/CD pipelines.
C.4. Problem Management	Ensuring cyber resilience and recovery, especially because ransomware attacks can shut down public services and damage data; operational continuity planning and rapid response mechanisms; responding to incidents, finding the root cause, and fixing the problem.
C.5. Systems Management	Performing threat modelling and designing secure Application Programming Interfaces (APIs); secure cloud environments by setting the right access controls, detecting threats, and making sure systems follow security standards and laws; applying security best practices to physical systems connected to the internet; managing backups and systems that help recover after a disruption,
D.12. Security Consulting	Identify and assess cybersecurity risks, decide which ones matter most, and make sure their security strategy supports business goals and follows legal requirements; translate complex cybersecurity issues to board-level decision-making; explaining cloud-related security risks in terms that business leaders understand; identifying, explaining technical risks in clear, business-focused language; explain cybersecurity issues to non-technical

	stakeholders, including board members, users, and external partners; clearly convey complex cybersecurity issues to various audiences, including non-technical stakeholders and executive leadership.
D.7. Science and Analysis	Dealing with ethical data issues; using AI or machine learning to detect unusual behaviour or patterns in data; critically reviewing AI results for bias, false alarms, or limitations; analysing what happened after an attack, collecting digital evidence, and using that information to prevent future incidents.
D.9. Personnel Development	Leading organisation-wide efforts to improve security awareness and responsibility.
E.3. Risk Management	Recognising deepfakes and synthetic voices used in phishing and social engineering campaigns; risk analysis and compliance with rules like NIS2; take responsibility in critical situations and navigate decision-making processes; analyse complex threats, challenge assumptions, and develop appropriate responses based on sound reasoning within complex public sector environments; detect, investigate, and respond to cyber incidents.
E.4. Relationship Management	The ability to work across departmental, organisational and disciplinary boundaries, including with external vendors; the ability to work across departmental, organisational and disciplinary boundaries, including with external vendors.
E.6. Quality Management and Compliance	Ensuring compliance with regulations such as NIS2.
E.9. Information Systems Governance	Recognise and act upon the ethical dimensions of cybersecurity; the ability to address complex supply chain dependencies, which heighten the risk of cyberattacks and complicate regulatory compliance; awareness of ethical implications in cybersecurity actions, and the ability to act with integrity and accountability.

Table AD. Most frequently mentioned competency content in the focus groups

4.4 Summarisation expected future needs

The combined insights from the vacancy analysis, trend reports, literature review, and focus groups offer a comprehensive overview of the cybersecurity labour market in Europe. EU-funded initiatives such as REWIRE, CyberSecPro, and CONCORDIA aim to bridge the gap between education and industry needs by developing job profiles, training programmes, and competence frameworks. Despite these efforts, challenges remain due to fragmented stakeholder collaboration, a shortage of qualified educators, and limited resources. The rapidly evolving threat landscape—driven by AI-powered attacks, geopolitical instability, and regulatory shifts like NIS2—requires cybersecurity professionals to possess a dynamic mix of hard and soft skills, including risk management, secure software development, and cross-functional communication. Across all trends, cybersecurity professionals must integrate technical expertise with strategic, legal, and communication skills to effectively manage emerging threats and regulatory demands. Focus group findings reinforce these needs, emphasising the importance of practical, hands-on learning, early exposure to cybersecurity, and the integration of ethical and interdisciplinary approaches. Key recommendations include strengthening soft skills, leadership, and communication, promoting inclusive education, and enhancing cooperation between industry, government, and academia to better align education with real-world cybersecurity demands.

An overall analysis was conducted in which the trends and developments from the trend reports, literature review, and focus groups were linked to the competences they impact. Based on how frequently each trend was mentioned across these sources, an adjustment factor was determined for all competences. The adjustment was calculated as follows: country reports: every point = +1%; literature review: every point = +3%; trend analysis: every point = +2,5%;

focus groups: every point = +2%. The results and adjustment factor are summarised in Table AE. This adjustment is later added to the vacancy-analysis based competence need. The adjustment factor represents the percentage by which we increase the demand for competences as calculated in the vacancy analysis, taking into account the trends mentioned in the country report, trend analysis, and focus groups. The higher the percentage, the more frequently the trend is mentioned and the more highly the competency is valued.

Identified number of trends requiring competence	**Cyber hubs - country reports**							**Literature review**	**Trend analysis**	**Focus groups**	**Adjustment factor**
	Lithuania	Spain	Estonia	Slovenia	Greece	Hungary	Belgium				
A.1. IS and Business Strategy Alignment										1	**2%**
A.2. Service Level Management											0%
A.3. Business Plan Development											0%
A.4. Product/Service Planning											0%
A.5. Architecture Design				1				1	2		**8%**
A.6. Application/Product Design										1	**2%**
A.7. Technology Trend Monitoring										1	**2%**
A.8. Sustainability Management											0%
A.9. Innovating											0%
A.10. User Experience											0%
B.1. Application/Product Development									2	1	**7%**
B.2. Component Integration		1	1								**2%**
B.3. Testing					2			6	1		**21%**
B.4. Solution Deployment											0%
B.5. Documentation Production		1	1								**2%**
B.6. ICT Systems Engineering	1	3	2	1	2	1	1		1		**14%**
C.1. User Support											0%
C.2. Change Support											0%
C.3. Service Delivery											0%
C.4. Problem Management	1	3	2	1	2			4	2	1	**28%**
C.5. Systems Management	2	2	2	1	2	1	2	4	1	1	**29%**
D.1. Information Security Strategy Development								2			**6%**
D.2. Quality Strategy Development											0%
D.3. Education and Training Provision								6	2		**23%**
D.4. Purchasing											0%
D.5. Sales Development											0%
D.6. Digital Marketing											0%
D.7. Science and Analysis			1						4	1	**13%**
D.8. Contract Management											0%
D.9. Personnel Development								5		1	**17%**
D.10. Information and Knowledge Management								1			**3%**
D.11. Needs Identification											0%
D.12. Security Consulting									1	1	**5%**
E.1. Forecast Development											0%
E.2. Project and Portfolio Management											0%
E.3. Risk Management		2	2		1			4	2	1	**24%**
E.4. Relationship Management									2	1	**7%**
E.5. Process Improvement											0%
E.6. Quality Management and Compliance	1	1	1		1	1			4	1	**17%**
E.7. Business Change Management								1	1		**6%**
E.8. Information Security Management		1	1		1	1	1	4			**17%**
E.9. Information Systems Governance	1		1				1			1	**5%**

Table AE. Expected future needs based on country reports, literature, trends and focus groups. Numbers are the number of trends that require the competence. The percentage is calculated as the sum of country reports (every point = +1%); literature review (every point = +3%); trend analysis (every point = +2,5%) and focus groups (every point = +2%). "The weighting percentages were assigned in this manner based on the volume and depth of the data analysed.

5 EDUCATION, COURSE & TRAINING OFFERINGS

5.1 Current education, course & training offerings

To analyse the cybersecurity education, course and training supply in the Netherlands, Greece, Cyprus and Croatia it was chosen to conduct research into different educational offerings, as these show the direct supply side of each country's education- and training market. The difference between an education, course or training programme lies in the duration and accreditation. An education programme takes a minimum of one year, after which a formal degree is provided. A course takes a minimum of five hours, after which the individual usually receives a formal certificate. A training usually takes between one to five hours, after which the individual can receive a certificate of participation or completion. Similarly to the needs analysis, the adjusted e-CF and ECSF roles are utilised. From each education, course or training required competences are extracted, which are matched to ECSF roles. Each ECSF role contains multiple competences. Education, courses and trainings can provide multiple ECSF roles relevant competence development. The combination of competences provides a percentual score regarding the size of overlap with the ECSF roles. Often, competences of several roles are combined into an education programme, course or training. After each individual country's supply side is identified from the analysis, an overarching analysis is conducted to show overlap in competences, roles and offerings.

5.1.1 The Netherlands

Total education, course & training offerings

The analysis of cybersecurity-related education, course and training offerings in the Netherlands for the period 2024–2025 includes in total 144 educational offers. The number of competences with proficiency level (1-5) present within total of educational offerings shows a covering of all domains (Plan (A), Build (B), Run (C), Enable (D) and Manage (E) with most presented E (level 2, 3, 4, 5) (see Table 29). Cybersecurity programmes in the Netherlands, spanning both public and private educational offerings, emphasise a well-rounded set of core competences aligned with industry needs. The most prevalent competence is 'E.8. Information Security Management', featured in 63,27% of programmes (see Table 30), with a balanced delivery across classroom (11,41%), online (14,81%), and hybrid (13,01%) formats (see Table 31). 'E.3. Risk Management' follows closely, integrated into 43,54% of offerings (see Table 30), with a strong online (10%) and hybrid (9,59%) presence (see Table 31). 'B.3. Testing' is also prominent, appearing in 29,93% of programmes, reflecting the importance of validating systems and defences (see Table 30).

Other frequently addressed areas include 'E.6. Quality Management and Compliance' (29,25%), 'C.5. System Management' (28,57%) and 'C.4. Problem Management' (26,53%), all of which support the operational and regulatory aspects of cybersecurity (see Table 30). More advanced or specialised topics such as 'D.7. Science and Analysis' (23,13%), 'A.5. Architecture Design' (21,09%), and 'A.7. Technology Trend Monitoring' (21,09%) are also represented, indicating a forward-looking approach that prepares learners for evolving technological landscapes (see Table 30). This distribution highlights a strong emphasis on both foundational and strategic cybersecurity skills across educational formats in the Netherlands.

Education programmes

An analysis of public education programmes reveals that universities and colleges place strong emphasis on strategic, operational, and analytical competences. The 26 analysed public education programmes (see Table 32) indicate the five highest competences offered: 'B.1. Application/Product Development' (27,42%), 'E.8. Information Security Management' (27,42%), 'A.7. Technology Trend Monitoring (24,19%), 'D.7. Science and Analysis (24,19%) and 'A.6. Application/Product Design' (19,35%) (see Table 33). The education programmes exhibit a robust basis in practical, hands-on abilities, reflected in B.1. Application/Product Development' and 'A.6. Application/Product Design'. Foremost among these is the development of practical skills in application development (B.1.). Many programmes also offer in-depth training in systematically identifying vulnerabilities, analysing trends and evaluating security management measures and indicators (E.8.). Additionally, data science, analytics, and the application of LLMs and AI have become increasingly prominent in curricula. Educational institutions are actively aligning their programmes with these emerging competences to stay relevant to labour market demands, and this trend is expected to continue growing. Interestingly, the competence of personnel development (D.9.) does not emerge as prominent. This can be explained by the fact that it is often integrally embedded within substantive cybersecurity modules.

Courses & trainings

The cybersecurity courses and training programmes (62 courses and 56 trainings) shows similarities in competences (see Table 34 and Table 36). In particular, 'E.8. Information Security Management' has a respective match of 54,84% and 73,21% for courses and trainings. Similarly, it can be seen that 'E.3. Risk Management' has a respective match of 43,55% and 44,64% (see Table 35 and Table 37). Furthermore, 'C.4. Problem Management' (30,65%), 'B.3. Testing' (29,03%) and 'E.6. Quality Management and Compliance' (29,03%) are highly matched competences for the analysed courses (see Table 35). Within the analysed trainings the same competences come forth but in a different order of matching percentages: 'B.3. Testing' (28,57%), 'E.6. Quality Management and Compliance' (28,57%) and 'C.4. Problem Management' (25,00%) (see Table 37).

Private cybersecurity programmes in the Netherlands place a strong emphasis on both strategic, operational, and analytical competences. At the forefront is 'E.8. Information Security Management', which ensures that learners are equipped to oversee and implement robust security frameworks. 'E.3. Risk Management' and 'B.3. Testing' are also central, reflecting the sector's focus on identifying vulnerabilities and validating system integrity. 'E.6. Quality Management and Compliance' is highly visible within the curricula of courses and trainings thereby ensuring alignment with regulatory standards. Notably, 'C.4. Problem Management' especially in combination with C.5. Systems Management (22,58% for courses; 21,43% for trainings) highlight the importance of effective incident resolution within operational systems (see Table 35 and Table 37). More advanced competences such as 'D.7. Science and Analysis' (20,97% for courses;10,71% for trainings) and 'D.1. Information Security Strategy Development (22,58% for courses; 17,86% for trainings) prepare professionals to engage in research-driven decision-making and long-term planning. Finally, 'E.9. Information Systems Governance' (20,97% for courses; 19,64% for trainings) underscores the need for oversight and accountability in managing complex IT environments (see Table 35 and Table 37).

ECSF roles

A large differentiation is evident when it comes to the matching between competences and ECSF roles. The top five roles for the education sector in the Netherlands are Cyber Threat Intelligence Specialist (4,50%), Cybersecurity Risk Manager (3,57%), Cybersecurity Researcher (1,09%), Penetration Tester (0,82%) and Cyber Incident Responder (0,82%) (see Table 38). As 'D.7. Science and Analysis' and 'E.8. Information Security Management' are relatively high matching competences, it is logical that Cyber Threat Intelligence Specialist has gained the highest percentual ECSF role match. Similarly, 'E.3. Risk Management' is a highly sought-after competence, which is reflected in the role of Cybersecurity Risk Manager. The largest differentiation can be seen between the top two ECSF roles and Cybersecurity Researcher, Penetration Tester and Cyber Incident Responder. One of the reasons why the ECSF role match is approximately 1% or lower, lies in the total number of labelled competences (770). For example, the number of competences that have been labelled in the Dutch vacancy analysis is 1380 and consequently enhance the ECSF role match.

5.1.2 Greece

Total education, course & training offerings

The analysis of cybersecurity-related education and training offerings in Greece for 2024 identified 47 programmes. Coverage spans all e-CF domains—Plan (A), Build (B), Run (C), Enable (D), and Manage (E)—with emphasis on D (Enable) and B (Build) when counting level-specific learning outcomes ("hits"). Across all mapped outcomes (n=506), domain distribution is: D 29.25%, B 25.49%, E 22.92%, A 19.96%, C 2.37%. Proficiency levels emphasise advanced learning targets: Level 4 47.04%, Level 3 40.32%, Level 5 9.88%, Level 2 2.77%, Level 1 0%.

The gathered dataset recorded 21 "Education" (formal) programmes and 26 "Course" (non-formal) offerings; delivery is either Online (21 cases), Hybrid (8 cases), Classroom (4 cases) or unspecified/changing based on groups (14 cases). Language of instruction is predominantly Greek. Non-formal offerings concentrate around a median workload of 40 hours (mean ≈ 37.7; min 14). Provision is geographically centred in Athens, complemented by online/hybrid modes. As noted in the Greek CyberHubs national report, no standalone undergraduate degrees in cybersecurity exist; supply is concentrated at EQF-7/8 and in a sizable ecosystem of non-formal (short-course/certification) training supported by universities, corporate academies, and professional associations (e.g., ISC2/ISACA).

The analysis of the most prevalent competences across Greek cybersecurity programmes shows that the basics needed for the **D.12 Security Consulting** role are universally covered by all cybersecurity programmes -either by providing specific in-programme specialty courses or by their general corpus- appearing in all forty-seven programmes assessed (100%). This is followed by E.3 Risk Management, which is present in thirty-four programmes (72.3%), and B.3 Testing, included in thirty-three programmes (70.2%). Three competences—E.8 Information Security Management, A.7 Technology Trend Monitoring, and B.5 Documentation Production—appear in thirty programmes each, representing 63.8% of the total. D.1 Information Security Strategy Development is identified in twenty-two programmes (46.8%). Finally, four competences—A.5 Architecture Design, A.6 Application Design, B.6 ICT Systems Engineering,

and B.1 Application Development—are each included in nineteen programmes (40.4%), while E.9 Information Systems Governance appears in fifteen programmes (31.9%).

Certain competences dominate the Greek education landscape. D.12 Security Consulting reflects the expectation that graduates can provide enablement and advisory functions, translating regulatory and assurance requirements such as NIS2 and DORA into actionable controls, implementation roadmaps, and strategic advice. The strong presence of E.3, E.8, and E.9 underlines the importance of governance, risk management, and information security management in sectors like finance, telecommunications, and energy, where formalised ISMS practices are critical. The prominence of B.3 Testing highlights the market's demand for assurance and secure software. Meanwhile, competences such as A.5, A.6, B.1, and B.6 indicate meaningful exposure to design and build activities, preparing learners to contribute to platform modernisation and product security, although the depth of coverage varies between providers and programme types.

Education programmes

An analysis of public/academic programmes (n=21) shows a marked focus on strategic, enablement, and governance competences, complemented by assurance and emerging technology themes. The five most prevalent competences are D.12 Security Consulting (100.0%), E.3 Risk Management (95.2%), A.7 Technology Trend Monitoring (95.2%), B.5 Documentation Production (85.7%), E.8 Information Security Management (81.0%), D.1 Information Security Strategy Development (66.7%) and B.3 Testing (57.1%).

Greek MSc curricula maintain a governance-first and enablement-centric design, with substantial risk/ISMS training and explicit trend literacy. Consulting-style outputs (policy sets, procedures, metrics) are reinforced by documentation competence. Assurance and analytics tracks are present and growing, aligning with the national report's observation that data/AI elements are increasingly embedded. This blend prepares graduates for roles that shape policy, architecture decisions, and programme-level security outcomes.

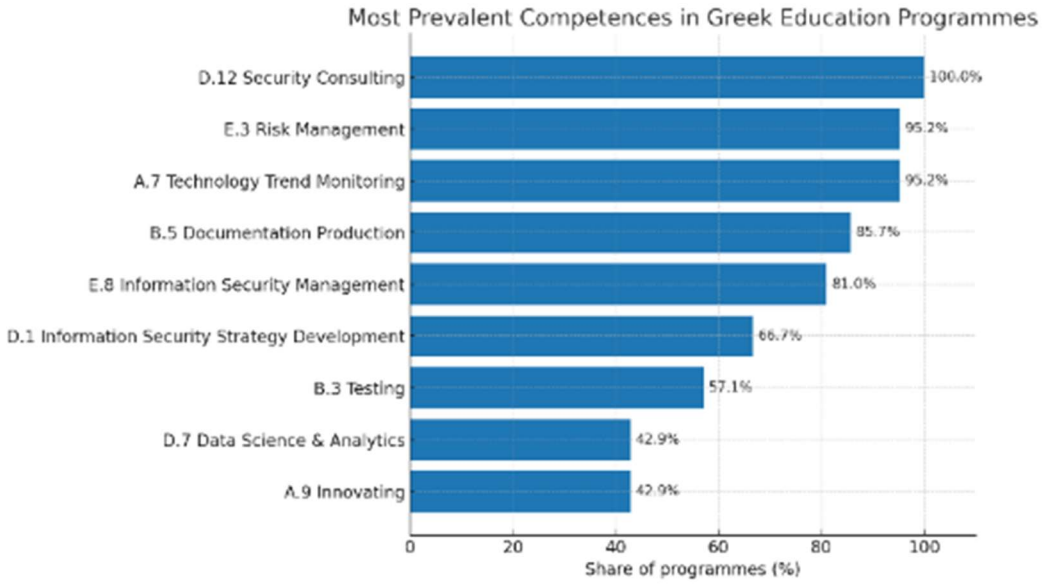

Figure 6. Most prevalent Competences in Greek Training Initiatives (n=47).

Greek MSc curricula maintain a governance-first and enablement-centric design, with substantial risk/ISMS training and explicit trend literacy. Consulting-style outputs (policy sets, procedures, metrics) are reinforced by documentation competence. Assurance and analytics tracks are present and growing, aligning with the national report's observation that data/AI elements are increasingly embedded. This blend prepares graduates for roles that shape policy, architecture decisions, and programme-level security outcomes.

Courses and trainings

For non-formal courses (n=26), the competency profile shifts toward hands-on build and testing while retaining governance essentials. The highest match still is D.12 Security Consulting (100.0%), followed by B.3 Testing (80.8%), E.3 Risk Management (53.9%) and E.8 Information Security Management (50.0%), A.5/A.6/B.6/B.1 (50.0% each), and B.5 (46.2%), A.7 (38.5%).

Greek private provision prioritises secure SDLC pipelines, validation, and engineering alongside advisory skills. This cluster is particularly aligned to implementation-heavy labour-market needs (secure design, platform hardening, control deployment).

Figure 7. Coverage of ECSA roles in Greek Training Courses (n=47).

ECSF roles

Concerning the coverage of ECSF roles (aggregate view across all 47 programmes) at all-programme level (see Fig. 5 above), the distribution evidences a balanced supply: strong governance/audit capacity (Cybersecurity Auditor (51.1%), Digital Forensics Investigator (46.8%), especially in formal programmes) and engineering/assurance strength (Cybersecurity Architect / Implementer / Penetration Tester (40.4% each), especially in non-formal courses). Together they align with the Greek vacancy landscape characterised by high demand for Cybersecurity Architect/Implementer, sustained DFIR/Pentest demand, and a material GRC layer.

Insights in education/training offers

Greek training programmes provide a 100% match in D.12 competence-coverage together with an ECSA Cybersecurity Risk Manager coverage in about 12.8% of programmes at ≥50% role match). This is due to the fact that ECSF roles require a constellation of competences (e.g., Risk Manager typically needs solid E.3 Risk Management, plus E.8 ISMS, E.9 Governance, D.1 Security Strategy, often E.6 Quality, etc., at sufficient proficiency and weight), having D.12 present (consulting/enablement) does not by itself push a programme over the ≥50% threshold for the Risk Manager role. Many programmes do cover E.3 and E.8, but don't combine enough of the other role-defining competences—or not at the required levels—to cross the threshold.

This pattern is reasonable for Greece since Greek programmes are very strong on Enable/Build and GRC fundamentals:

- D.12 (Consulting) 100%, E.3 (Risk) 72.3%, E.8 (ISMS) 63.8%.

- But E.9 (Governance) and D.1 (Security Strategy), which are key to the Risk Manager role, are present in fewer programmes (31.9% and 46.8%, respectively).
- Result: many curricula are advisory-capable and risk/ISMS-aware, but not all meet the full ECSF bundle for Risk Manager at the ≥50% threshold.

A programme can teach consulting (D.12)—client-facing enablement—without offering the full risk-management leadership package (policy governance, metrics, audit interfacing, enterprise risk integration, strategy, etc.) at the required depth/weights to earn a ≥50% match for Risk Manager. Non-formal courses tend to emphasise hands-on build/testing (e.g., B.3, A.5/A.6/B.1/B.6) and practical enablement (D.12), which improves Architect/Implementer alignment more than Risk Manager alignment. Formal Education programmes push governance/strategy further, but still not universally enough to lift Risk Manager over 50% in large numbers.

For training strategies, the targeted survey highlighted the following as most relevant and effective:

- Upskilling existing ICT personnel.
- On-the-job coaching and training.
- In-company training by external providers.
- Reskilling non-ICT personnel.
- In-company training by own staff.
- External training.

These insights offer a comprehensive foundation for shaping future training programmes and aligning them with real-world needs across sectors.

5.1.3 Cyprus

In Cyprus, 13 education and training offerings from 2024-2025 have been included (see Table 47). In particular, 4 education offerings and 9 trainings are analysed (see Table 50 and Table 52). All of the education programmes refer to postgraduate level. For the education market analysis of Cyprus, no courses have been analysed as no course-type entries were identified in the dataset.

General findings

The analysis of cybersecurity-related education and training offerings in Cyprus for the period 2024–2025 reveals a focused but selective approach to competence development. A total of 13 offerings were reviewed, including formal academic programmes and professional training initiatives. These offerings reflect a growing awareness of the need to build national cybersecurity capacity, though the scope and depth of competences addressed vary significantly across programmes of study. Interestingly, despite the strategic focus evident in the selection of competences, foundational-level skills (e-1 and e-2) are not widely covered (see Table 47). The majority of training is provided at intermediate proficiency levels (particularly e-3), which corresponds to roles requiring the ability to apply cybersecurity concepts independently in real-world settings. Only a small portion of training reaches the higher

proficiency levels (e-4 or e-5), such as those needed for senior management, architectural, or governance roles.

Total education & training offerings

The most commonly addressed competences across the reviewed offerings include:

- Risk Management (E.3.) – featured in 69.2% of offerings
- Technology Trend Monitoring (A.7.) – 38.5%
- Information Systems Governance (E.9.) – 38.5%
- ICT Systems Engineering (B.6.) – 23.1%
- Information Security Strategy Development (D.1.) – 23.1%.

'D.1. Information Security Strategy Development' (23,08%) (see Table 48) indicates a strong emphasis on strategic foresight, governance, and operational resilience, aligning with broader national priorities in cybersecurity. Most competences are delivered at intermediate proficiency levels, supporting the development of professionals who can operate independently in technical and analytical roles.

While Cyprus's cybersecurity training offerings demonstrate alignment with high-demand areas, some important competences remain underrepresented (see Table 52 and Table 53). First, 'D.3. Education and Training Provision' competences, such as those needed to prepare new cybersecurity professionals or to build internal training capacity, are absent. Second, 'C.1. User Support' and 'B.5. Documentation Production' —key to ensuring the effective dissemination of cybersecurity knowledge and operational continuity—are addressed in only one training each. This is particularly concerning for smaller organisations and public institutions, which often rely heavily on in-house teams for incident handling and user education. Third, advanced analytics and data-driven competences like 'D.7. Science and Analysis' are marginally addressed (only one training at e-2), which may limit the ability of future professionals to engage with data-rich threat intelligence or AI-based security solutions.

There is a strong degree of alignment between education offerings and the most in-demand competences identified in the job vacancy analysis (see Table 50 and Table 51). In particular, the following competences are frequently addressed in both education and employment contexts:

- Risk Management;
- Technology Trend Monitoring;
- Information Security Strategy Development.

This alignment suggests that education providers are responsive to national workforce needs, especially in areas that support strategic planning and threat anticipation. Despite this alignment however, several gaps remain. Competences related to education and training provision, user support, and documentation—while prominent in job vacancy requirements—are less frequently addressed in current offerings. This indicates a need for more targeted programmes that support internal capacity building, operational continuity, and knowledge management, particularly within small and medium-sized enterprises and public institutions. Most of the reviewed training offerings in Cyprus are delivered online, with a smaller portion available in classroom or hybrid formats (see Table 49). This delivery model is particularly suited to working professionals seeking to upskill without disrupting their careers and also benefits

geographically dispersed learners. However, it also implies that hands-on, practical training may be limited unless specifically integrated into the curriculum design.

ECSF roles

The Cyprus education and training landscape demonstrates the strongest alignment with only one role: Cyber Threat Intelligence Specialist (3,16%) (see Table 54). This suggests a clear emphasis on research, governance and information management dimensions of cybersecurity education. However, the absence of alignment with roles like Chief Information Security Officer, Cybersecurity Architect, and Penetration Tester highlights a gap in strategic, architectural, and offensive security training. This points to a need for future programme development to address higher-level leadership and technical specialisations within the cybersecurity domain. Concluding, as no additional matches have been identified from the ECSF role analysis, this clearly shows a lack of competence supply.

5.1.4 Croatia

Total education, course & training offerings

The cybersecurity education, course and training framework in Croatia for 2024–2025 includes 64 formal education programmes, (see Table 58), 23 courses (see Table 60), and 5 specialised training options (see Table 62), totalling to 92 offerings (see Table 55). These efforts collectively demonstrate a robust emphasis on developing technical and operational competences associated with the Build (B) and Run (C) domains of the e-Competence Framework. The most commonly identified competences encompass 'D.7. Science and Analysis' (67,39%), 'C.5. Systems Management' (66,30%), 'B.1. Application/Product Development' (63,04%) and 'E.8. Information Security Management' (61,96%) (see Table 56). The predominant offers are focused on skill levels e2 (231) and e3 (514), signifying a robust alignment with equipping practitioners for entry-level and mid-level operational positions. Nevertheless, competences at e-4 (182) and e-5 (8)—crucial for strategic planning, governance, and leadership positions—are infrequently emphasised, especially in non-formal training and course formats (see Table 55). Although core technical competences are adequately addressed, there is a significant deficiency in provisions concerning legal, compliance, governance, and innovation-related domains (e.g., 'E.9. Information Systems Governance', 'A.9. Innovating' and 'D.2. Quality Strategy Development'), which are becoming increasingly pertinent in the advancing cybersecurity landscape. This indicates a necessity for diversification and enhancement of the existing portfolio to incorporate advanced, interdisciplinary competences.

Education programmes

The 64 education programmes exhibit a robust basis in practical, hands-on abilities, with 'B.1. Application/Product Development' being the most prevalent competence, represented in 89,06% of all programmes. Other prominently featured competences are 'C.5. Systems Management' (75%), 'D.7. Science and Analysis (75%), 'A.6. Application/Product Design (54.7%), and 'A.5. Architecture Design' (64,06%) (see Table 59). This signifies a curriculum centred on technical cybersecurity execution, system upkeep, and analytical reasoning. The education system seems to be structured to provide the national labour market with individuals equipped to assume essential operational and engineering positions. Strategic and managerial competences, including 'A.1. IS and Business Strategy Alignment', 'E.7. Business Change Management', and 'E.9. Information Systems Governance', are incorporated in fewer than 20%

of programmes, indicating a deficiency in preparation for senior or leadership positions in cybersecurity (see Table 59). Furthermore, competences in domains such as 'A.8. Sustainability Management', 'A.9. Innovating', and 'D.6. Digital Marketing' are largely lacking, indicating a conventional, technically focused structure of education programmes (see Table 59).

Courses

Among the 23 courses analysed, a pattern observed in formal education persists, albeit with an intensified focus on practical and implementation abilities. The primary competences encompass 'E.8. Information Security Management' (60.87%), 'D.7. Science and Analysis' (52,17%), 'C.5. Systems Management' (47.83%), 'B.3. Testing (43.48%) and 'C.4. Problem Management' (43,48%) (see Table 61). Courses are well-suited to facilitate applied learning, particularly for workers transitioning into cybersecurity positions or enhancing their skills inside technical teams. Nonetheless, like training, advanced competences in planning, leadership, and governance are often inadequately represented. Few courses cover A-level (Plan) competences, and domains such as 'D.5. Sales Development', 'A.9. Innovating', or 'E.7. Business Change Management' are largely absent (see Table 61). That indicates a robust technological base in course offerings, although a constrained scope for strategic or interdisciplinary advancement.

Trainings

Only five specialised training programmes were in the dataset, indicating a concentrated approach. The competences most commonly addressed are 'D.12. Security Consulting' (100%), 'B.5. Documentation Production' (80%), 'E.9. Information Systems Governance' (80%), 'C.4. Problem Management (60%), 'E.3. Risk Management' (60%), 'E.6. Quality Management and Compliance' (60%) and 'E.8. Information Security Management' (60%) (see Table 63). These trainings are specifically designed to enhance the skills of professionals in positions that necessitate documentation precision, advisory proficiency, incident response, and regulatory compliance. Their focus is on mid-to-high-level competences (mostly at e-3 and e-4), suggesting that training is used to close gaps for seasoned practitioners rather than to cultivate entry-level skills. The low availability of training alternatives and their narrow thematic focus indicate a deficiency in agile and ongoing professional development pathways, particularly in emerging areas such as cyber law, AI-driven security, and cloud governance.

ECSF roles

The Croatian education, course and training ecosystem exhibits the most significant alignment with roles, including Cybersecurity Risk Manager (4,95%), Cyber Threat Intelligence Specialist (3,08%), Cybersecurity Researcher (2,64%), Cyber Incident Responder (2,42%) and Penetration Tester (1,32%), when mapped to the ECSF (see Table 64). These alignments indicate that the current education, course and training offerings sufficiently support workforce preparedness for technical, operational, and knowledge-sharing roles. However, roles requiring comprehensive system-wide management and leadership—such as Chief Information Security Officer, Cyber, Legal, Policy & Compliance Officer or Cybersecurity Auditor—are inadequately represented, highlighting the necessity for enhanced emphasis on strategic and governance-related competences in forthcoming programme development.

Conclusion

The examination of cybersecurity education, course and training provisions in Croatia reveals a robust framework for cultivating technical and operational competences, particularly through

formal education programmes. These programmes are specifically intended to equip professionals for positions centred on implementation, systems management, and information security operations, aligning with the mid-level proficiency spectrum (e-2 and e-3). Nonetheless, a significant deficiency exists in programmes targeting advanced strategic competences, particularly those associated with planning, governance, compliance, and innovation. Advanced subjects, such as business strategy alignment, risk governance, and legal and regulatory frameworks, are often overlooked, especially in training programmes and short-format courses. This disparity hinders the influx of experts qualified for leadership, policy, or critical advisory positions in cybersecurity.

Moreover, the alignment of instructional content with ECSF roles indicates that positions such as cybersecurity risk manager, cyber threat intelligence specialist, and cybersecurity researcher are adequately supported; however, essential roles like CISO, compliance officer, auditor, and policy-oriented positions are insufficiently addressed. The investigation highlights a structural challenge: although the e-CF provides a comprehensive structure for ICT competences, it often fails to capture the unique complexity and multidisciplinary nature of cybersecurity tasks. Numerous competences vital for security leadership, legal compliance, and national security obligations are inadequately articulated or dispersed throughout the framework. The ECSF role profiles provide more detailed descriptions of actual cybersecurity positions, although they have not been adequately integrated into the development of training and educational programmes. That highlights the necessity of enhancing the integration of ECSF-aligned role conceptualisation into curriculum development and maybe modifying the e-CF for increased pertinence in the cybersecurity sector. Such actions would facilitate the alignment of Croatia's education, course and training environment with the increasing demands and intricacies of the cybersecurity labour landscape.

5.2 Other countries & analyses

Building on the preceding country analyses, six educational databases originating from various EU projects have been identified (Table AF). These databases offer the potential to catalogue a wide spectrum of educational offerings, including professional courses, trainings, certifications, bachelor's and master's programmes, as well as broader university curricula. A closer look reveals that most of these databases tend to concentrate on university-level education. This finding reinforces CADMUS's targeted focus on SMEs and public professionals, thereby fulfilling current sector demands (Almeida, 2025). In particular, it has become increasingly clear from the needs analysis that a more tailored and diverse set of courses and trainings is needed to address the unique learning demands that are visible in the SME- and public sector.

Project	Scope	Countries	Number of courses / study programmes	Form
CONCORDIA	Professional courses	EU, Turkey, Israel	55	online: 10 blended: 7 face-to-face: 49
CyberSec4Europe	University curricula (Master only)	EU	200	unclear
CyberSecPro (CyberSecPro, 2022b, p.17-79)	Cybersecurity training course catalogue	EU	81	Academica lab courses: 48%

	Undergraduate courses (52%), graduate courses (20%), summer school courses (9%), professional training courses (19%)			Commercial seminars: 18% Cybersecurity exercises/tools: 34%
SPARTA	University curricula (Bachelor and Master)	EU, US, Canda, South Korea, Japan, Australia	137	Predominantly online, exact number unclear
ENISA	University curricula (Bachelor, Master, Postgraduate)	EU, EFTA	171	Online: 31 Classroom: 102 Blended: 38
REWIRE	Trainings, certifications	EU	64 trainings, 27 certifications	Online: 4

Table AF. Database of education for cybersecurity reporting scope and size amongst other.

Although the analysed EU projects focus mostly on university-level education, it has become evident from the databases that the majority of courses, bachelors and masters are being taught in a physical environment, instead of online. On the one hand, CONCORDIA and ENISA have a predominant focus on in-person programmes. On the other hand, most of the cybersecurity trainings from the SPARTA and REWIRE projects are delivered online (SPARTA, 2021, p.18; Delgado et al., 2023). The SPARTA project also notes that online education, particularly in the form of blog posts, has proven to be an effective approach. This method makes information broadly accessible to the public, regardless of academic enrolment status. Furthermore, this entails a self-learning component, which can enhance productivity.

The analysed EU projects further show that the delivery method of trainings and courses needs to be addressed to make education more practical. In particular, ENISA and the CyberHubs project by CyberSecPro emphasise the need for non-formal education. Gamification, situated learning, virtualisation, hackathons and simulations are all practical delivery methods. Each method can function as input for the training requirements and consequent development of CADMUS' trainings and courses. An example can be found in CONCORDIA's Cyber Range, which is a simulation room in which professionals can become more familiar with the practical side of cybersecurity issues. The requirements of CONCORDIA's Cyber Range, namely repeatability, scalability, automation and interoperability, are important factors to consider whilst looking at training requirements.

5.3 Summarisation education, course & training offerings

From the education market analysis it has become evident that in the Netherlands, Greece, Cyprus and Croatia the following competences are the most frequently addressed in education, course and training offerings: 'E.8. Information Security Management' (60,24%), 'E.3. Risk Management' (41,77%), 'C.5. Systems Management' (41,37%), 'D.7. Science and Analysis' (39,36%) and 'B.3. Testing' (33.73%) (see Table 67 and Figure 8). Interestingly, information security management, risk management and testing are also amongst the top five competences in the needs analysis, highlighting that both the demand and supply side have similar focuses. Furthermore, abilities in the realms of systems management and data analysis are frequently taught in education, course and training offerings. For example, within a cybersecurity or IT bachelor, C.5. and D.7. are essential competences to learn.

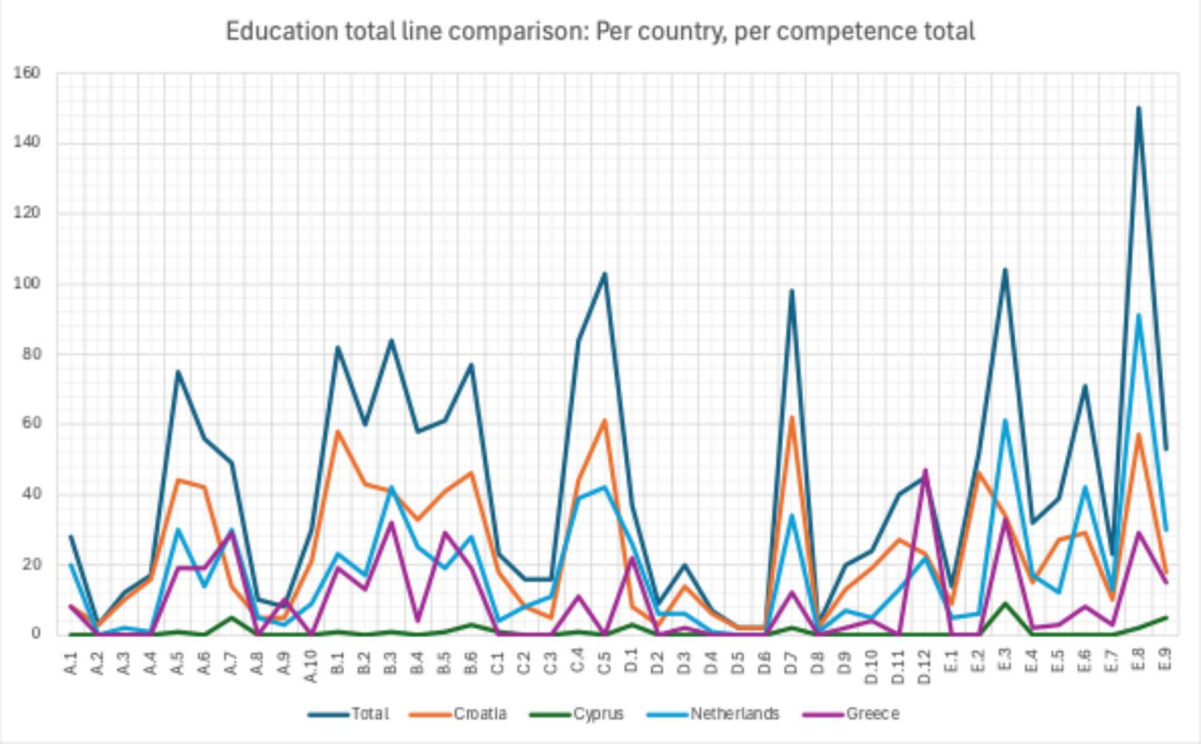

Figure 8. Amount of education, courses and trainings covering of competences, overall and per country.

Education programmes are for example bachelor's and master's that have a duration of one year minimum. Therefore, increasingly more competences can be distilled from these offerings. As education programmes are mostly gathered from general universities and universities of applied sciences it is logical that 'D.7. Science and Analysis' (25,70%) is amongst the top five competences. Students need to possess analytical thinking and writing skills to conduct proper (academic) research. Furthermore, 'B.1. Application/Product Development' (29,72%), 'C.5. Systems Management' (22,89%), 'E.8. Information Security Management' (22,89%), 'A.5. Architecture Design' (21,29%) (see Table 67) are competences related to the central topics within an education programme. For example, bachelor's in software engineering teach application development and -design and system management skills. Other bachelors that are focused on cybersecurity regularly teach information security principles.

Courses and trainings have a similar focus in terms of education market supply. Both courses and trainings focus respectively on 'E.8. Information Security Management' (19,28%; 18,07%), 'E.3. Risk Management' (14,86%; 14,06%), 'C.4. Problem Management' (11,65%; 7,23%) and 'B.3. Testing' (11,24%; 7,63%). The only difference can be seen regarding 'C.5. Systems Management' (courses: 12,05%) and 'E.6. Quality Management and Compliance' (trainings: 7,63%) (see Table 67). One of the functions of courses and trainings is to reward individuals with specific certifications. For example, the CISM and CISSP certifications are closely related to, respectively, information security management and systems- and problem management.

Regarding the ECSF roles, it is shown that the matching percentages are relatively low, even lower than the needs analysis. The top five ECSF roles are Cyber Threat Intelligence Specialist

(3,58%), Cybersecurity Risk Manager (2,84%), Cybersecurity Researcher (1,24%), Cyber Incident Responder (1,08%) and Penetration Tester (0,71%) (see Table 68). A possible explanation for the low matching percentages lies in the curricula of education, course and training offerings. Trainings and courses usually focus on one or two topics within their curricula. As ECSF roles encompass a wide variety of competences, it is likely that only one or two competences are matched between trainings/courses and ECSF roles.

6 GAP ANALYSIS

6.1 Key-findings gap analysis

The table below (Table AG) presents a summary of the key gaps between the demand for competences—based on the vacancy analysis, country reports, trend analysis, and focus groups—and the supply of competences in educational programmes. Green highlights indicate the main priorities for investing in educational offerings, where demand for competences exceeds supply. Red indicates areas where the supply in education is greater than the demand.

	GAP in %						
Competence/ Proficiency level	**Level e-1**	**Level e-2**	**Level e-3**	**Level e-4**	**Level e-5**	**Overall**	**Rank Overall**
A.1. IS and Business Strategy Alignment				-2%	1%	-4%	24
A.2. Service Level Management			0%	0%		-1%	9
A.3. Business Plan Development			-2%	-1%	-1%	-4%	25
A.4. Product/ Service Planning		-4%	-1%	0%		-6%	27
A.5. Architecture Design			-5%	2%	7%	-12%	34
A.6. Application/ Product Design	0%	-5%	-9%			-17%	40
A.7. Technology Trend Monitoring			-6%	2%	1%	-7%	28
A.8. Sustainability Management			-3%	0%		-3%	22
A.9. Innovating				-2%	0%	-3%	19
A.10. User Experience		-4%	-5%	-1%		-10%	32
B.1. Application/ Product Development	5%	1%	-12%			-20%	41
B.2. Component Integration		-6%	-8%	2%		-16%	37
B.3. Testing	16%	18%	9%	17%		-1%	10
B.4. Solution Deployment	-4%	-2%	-9%			-15%	36
B.5. Documentation Production	2%	1%	-7%			-8%	29
B.6. ICT Systems Engineering			-4%	8%		-10%	30
C.1. User Support	-3%	0%	-1%			-4%	23
C.2. Change Support		0%	-2%			-2%	16
C.3. Service Delivery	0%	-1%	-2%			-3%	20
C.4. Problem Management		23%	22%	21%		10%	3
C.5. Systems Management	24%	22%	10%			-1%	12
D.1. Information Security Strategy Development				4%	5%	3%	4
D.2. Quality Strategy Development				-2%	0%	-1%	14
D.3. Education and Training Provision		25%	21%			23%	1
D.4. Purchasing		-1%	0%	0%		-1%	13
D.5. Sales Development		0%	0%	0%		0%	6
D.6. Digital Marketing		0%	0%	0%		-1%	8
D.7. Science and Analysis		10%	-4%	3%	13%	-17%	38
D.8. Contract Management		0%	0%	0%		0%	7
D.9. Personnel Development		16%	13%	16%		11%	2
D.10. Information and Knowledge Management			-1%	1%	3%	-3%	21
D.11. Needs Identification			-9%	-2%	0%	-12%	33
D.12. Security Consulting			0%	2%		-3%	18
E.1. Forecast Development			-4%	-1%		-4%	26
E.2. Project and Portfolio Management		-9%	-6%	-2%	-1%	-17%	39
E.3. Risk Management		19%	13%	16%		0%	5
E.4. Relationship Management			0%	5%		-2%	15
E.5. Process Improvement			-9%	-3%		-12%	35
E.6. Quality Management and Compliance		16%	4%	12%		-2%	17
E.7. Business Change Management			0%	5%	5%	-1%	11
E.8. Information Security Management		4%	2%	5%		-22%	42
E.9. Information Systems Governance				-7%	2%	-10%	31

Table AG. Overall Gap Analysis per level. Based on country data, literature review, trend analysis, focus groups and vacancy analysis (n=606) and development offers (n=249). Green = Opportunities for education: demand exceeds the supply of current educational offers. Yellow = Education is on par with demand. Orange/Red = Surplus: the supply of current educational offers exceeds the demand in job vacancies now and in the future.

The five most important opportunities for expanding the educational offering are the competences ‘D.3. Education and Training Provision’ , ‘D.9. Personnel Development’, ‘C.4. Problem Management’, ‘D.1. Information Security Strategy Development’, and ‘E.3. Risk Management’. For these competences, the demand exceeds the supply of current educational offerings. This suggests that the main priority for education is not necessarily the more technical competences, but rather the strategic and business-oriented one. However, when breaking down the data by level, we observe that ‘C.4. Problem Management, ‘C.5. System Management’, ‘B.3. Testing’, ‘E.3. Risk Management’, and ‘E.6. Quality Management and Compliance’ also rank among the most significant gaps. This data highlights the necessity of taking a level-specific approach when determining where to invest in new educational offerings. The table below highlights the top 20 priorities to invest in; for these competences demand exceeds the supply of current educational offers (Table AH).

	Level e-1	Level e-2	Level e-3	Level e-4	Level e-5
A.1. IS and Business Strategy Alignment				91	46
A.2. Service Level Management			63	71	
A.3. Business Plan Development			86	74	77
A.4. Product/ Service Planning		100	80	67	
A.5. Architecture Design			103	41	24
A.6. Application/ Product Design	60	101	111		
A.7. Technology Trend Monitoring			106	38	45
A.8. Sustainability Management			92	67	
A.9. Innovating				89	71
A.10. User Experience		99	102	79	
B.1. Application/ Product Development	29	47	115		
B.2. Component Integration		104	109	42	
B.3. Testing	12	9	22	10	
B.4. Solution Deployment	96	85	112		
B.5. Documentation Production	40	43	107		
B.6. ICT Systems Engineering			98	23	
C.1. User Support	93	52	76		
C.2. Change Support		51	87		
C.3. Service Delivery	63	81	83		
C.4. Problem Management		3	5	6	
C.5. Systems Management	2	4	21		
D.1. Information Security Strategy Development				33	26
D.2. Quality Strategy Development				84	49
D.3. Education and Training Provision		1	7		
D.4. Purchasing		82	56	58	
D.5. Sales Development		61	56	58	
D.6. Digital Marketing		67	67	54	
D.7. Science and Analysis		20	97	34	18
D.8. Contract Management		62	49	63	
D.9. Personnel Development		14	17	11	
D.10. Information and Knowledge Management			78	44	35
D.11. Needs Identification			114	88	63
D.12. Security Consulting			55	39	
E.1. Forecast Development			95	75	
E.2. Project and Portfolio Management		110	105	90	73
E.3. Risk Management		8	16	13	
E.4. Relationship Management			53	27	
E.5. Process Improvement			113	94	
E.6. Quality Management and Compliance		15	32	19	
E.7. Business Change Management			48	30	28
E.8. Information Security Management		31	36	25	
E.9. Information Systems Governance				108	37

Table AH. Priorities for investment in education: rank most important gaps across levels (top 20 highlighted in green).

The gap analysis shows that there is only a small gap in areas such as ‘A.2. Service Level Management’, ‘A.4. Product/Service Planning’, ‘A.9. Innovation’, ‘D.11. Needs Identification’, ‘D.8. Contract Management’, ‘D.4. Purchasing’, ‘D.6. Digital Marketing’, ‘B.1. Application & Product Development’, and ‘D.2. Quality Strategy Development’. Here, the demand for competences appears to match the supply. These competences also do not emerge from the trend analysis and focus groups as areas expected to change significantly. Thus, supply and demand seem to be well aligned in these areas.

Regarding the competences ‘A.5. Architecture Design’; ‘C.4. Problem Management’; ‘B.4. Solution Deployment’; ‘C.5. Systems Management’; ‘E.9. Information Systems Governance’; ‘E.6. Quality Management and Compliance’; ‘B.3. Testing’; ‘E.3. Risk Management’; and ‘E.8. Information Security Management’, there is clearly more supply in educational programmes than demand from employers. However, this gap is not problematic in the short term, as several of these competences are prominently highlighted in the focus groups and trend analyses as becoming more important in the near future. In particular, ‘C.4. Problem Management’, ‘E.9. Information Systems Governance’, and ‘E.3. Risk Management’ are mentioned as competences that will become even more important going forward.

An important consideration when interpreting the competency gaps is the variation in demand between SMEs and public organisations. Among SMEs, the three most sought-after competences are ‘D.12. Security Consulting’, ‘C.5. Systems Management’, and ‘C.4. Problem Management’. In contrast, large public organisations primarily emphasise ‘D.12. Security Consulting’, ‘D.7. Science and Analysis’, and ‘E.4. Relationship Management’. Furthermore, evidence from other European studies suggests that SMEs tend to prefer informal learning methods and short-term training programmes.

An important remark by the data is specialist technical skills such as reverse engineering, virus analysis, and secure coding methods are essential in the cybersecurity field, despite not being officially categorised as distinct jobs or competences within ECSF. These skills are essential for positions such as threat hunters, malware analysts, and exploit developers—experts who function at the most fundamental levels of cyber protection and offense. The omission of these subjects in both ECSF role profiles and e-CF competences may convey a misleading message to training providers and policymakers, perhaps resulting in insufficient organised offers in these technically challenging domains.

Regarding the competences that are labelled red or dark orange in Table AG, these competences are well represented in the educational offerings we analysed. Through sharing these insights with schools, trainers and curriculum designers, we support them with evidence regarding (future) training needs. It is up to them to decide if and when to make adjustments or develop new offers.

6.2 Differences between types of education

Disaggregating the gap analysis by type of educational programmes—education, courses, and training—provides a more precise understanding of the discrepancies between competency demand and supply, as well as the strategic priorities for investing in cybersecurity education.

6.2.1 Education

For education, the top 20 gaps can be related to ten competences (see Table AI): 'A.5. Architecture Design', 'B.3. Testing', 'C.4. Problem Management, 'C.5. Systems Management', 'D.3. Education and Training Provision', 'D.7. Science and Analysis', 'D.9. Personnel Development', 'E.3. Risk Management', 'E.6. Quality Management & Compliance', and 'E.8. Information Security Management'. The five biggest gaps are:

1. Systems Management (C.5., Level 4)
2. Education and Training Provision (D.3., Level 2)
3. Risk Management (E.3., Level 2)
4. Education and Training Provision (D.3., Level 3)
5. Testing (B.3., Level 4)

	GAP in %					
Competence/ Proficiency level	**Level e-1**	**Level e-2**	**Level e-3**	**Level e-4**	**Level e-5**	**Overall**
A.1. IS and Business Strategy Alignment				-10%	2%	1%
A.2. Service Level Management			-1%	-2%		-1%
A.3. Business Plan Development			-6%	-2%	-2%	-3%
A.4. Product/ Service Planning		-11%	-4%	-1%		-6%
A.5. Architecture Design			-27%	-5%	10%	-3%
A.6. Application/ Product Design	-3%	-16%	-27%			-16%
A.7. Technology Trend Monitoring			-13%	-4%	3%	1%
A.8. Sustainability Management			-9%	-1%		-3%
A.9. Innovating				-6%	0%	-2%
A.10. User Experience		-9%	-16%	-3%		-10%
B.1. Application/ Product Development	0%	-10%	-42%			-17%
B.2. Component Integration		-17%	-23%	1%		-11%
B.3. Testing	10%	16%	9%	20%		18%
B.4. Solution Deployment	-10%	-10%	-7%			-5%
B.5. Documentation Production	-2%	-9%	-11%			1%
B.6. ICT Systems Engineering			-26%	8%		1%
C.1. User Support	-8%	-4%	-4%			-2%
C.2. Change Support		-3%	-4%			0%
C.3. Service Delivery	0%	-2%	-7%			-1%
C.4. Problem Management		14%	20%	27%		29%
C.5. Systems Management	18%	11%	8%			17%
D.1. Information Security Strategy Development				8%	7%	14%
D.2. Quality Strategy Development				-7%	0%	-1%
D.3. Education and Training Provision		22%	20%			27%
D.4. Purchasing		-5%	0%	0%		-1%
D.5. Sales Development		-1%	-1%	0%		0%
D.6. Digital Marketing		-1%	-1%	0%		-1%
D.7. Science and Analysis		8%	-21%	-7%	13%	-3%
D.8. Contract Management		1%	0%	0%		1%
D.9. Personnel Development		16%	7%	16%		14%
D.10. Information and Knowledge Management			-7%	1%	3%	0%
D.11. Needs Identification			-26%	-5%	0%	-9%
D.12. Security Consulting			-2%	2%		8%
E.1. Forecast Development			-7%	-1%		-2%
E.2. Project and Portfolio Management		-21%	-14%	-5%	1%	-12%
E.3. Risk Management		21%	15%	20%		29%
E.4. Relationship Management			-10%	5%		2%
E.5. Process Improvement			-26%	-6%		-10%
E.6. Quality Management and Compliance		16%	7%	11%		16%

E.7. Business Change Management			-5%	3%	5%	2%
E.8. Information Security Management		3%	-5%	14%		16%
E.9. Information Systems Governance				-10%	6%	4%

Table AI. Gap Analysis per level (incl. Total vacancy, CyberHub, Trends, Focus Groups) for all Education. Based on country data (Croatia, Cyprus, The Netherlands), vacancy analysis (n=606) and education offers (n=94).

6.2.2 Courses

In contrast to education and training, the competency gap profile for courses reveals a distinctly different pattern (see Table AJ). The top 20 gaps can be related to the competences: 'A.9. Innovating', 'B.2. Component Integration', 'B.3. Testing', 'B.6. ICT Systems Engineering', 'C.4. Problem Management', 'C.5. Systems Management', 'D.3. Education and Training Provision', 'D.5. Sales Development', 'D.7. Science and Analysis', 'D.9. Personnel Development', 'D.11. Needs Identification', 'E.2. Project and Portfolio Management', 'E.6. Quality Management and Compliance', and 'E.8. Information Security Management'. The five most important priorities for expanding the course offering are: (1) User Support (C.1., Level 1), (2) Problem Management (C.4., Level 2), (3) Systems Management (C.5., Level 2) and (4) Education and Training Provision (D.3., Level 2 and 3).

	GAP in %					
Competence/ Proficiency level	**Level e-1**	**Level e-2**	**Level e-3**	**Level e-4**	**Level e-5**	**Overall**
A.1. IS and Business Strategy Alignment				2%	-1%	5%
A.2. Service Level Management			0%	0%		0%
A.3. Business Plan Development			0%	0%	0%	1%
A.4. Product/ Service Planning		0%	0%	0%		1%
A.5. Architecture Design			6%	7%	8%	14%
A.6. Application/ Product Design	2%	3%	4%			5%
A.7. Technology Trend Monitoring			-3%	0%	0%	8%
A.8. Sustainability Management			1%	4%		1%
A.9. Innovating				12%	0%	0%
A.10. User Experience		0%	1%	0%		2%
B.1. Application/ Product Development	4%	8%	8%			12%
B.2. Component Integration		3%	0%	11%		6%
B.3. Testing	1%	17%	10%	0%		21%
B.4. Solution Deployment	0%	2%	-13%			2%
B.5. Documentation Production	0%	6%	-6%			11%
B.6. ICT Systems Engineering			9%	16%		17%
C.1. User Support	29%	4%	1%			6%
C.2. Change Support		1%	-2%			3%
C.3. Service Delivery	0%	-2%	2%			2%
C.4. Problem Management		29%	21%	0%		33%
C.5. Systems Management	0%	28%	4%			28%
D.1. Information Security Strategy Development				0%	4%	12%
D.2. Quality Strategy Development				0%	0%	2%
D.3. Education and Training Provision		26%	22%			29%
D.4. Purchasing		1%	-1%	-1%		1%
D.5. Sales Development		0%	0%	17%		1%
D.6. Digital Marketing		0%	0%	2%		0%
D.7. Science and Analysis		10%	1%	-1%	13%	12%
D.8. Contract Management		1%	0%	-1%		1%
D.9. Personnel Development		16%	18%	-1%		19%
D.10. Information and Knowledge Management			4%	-2%	3%	5%
D.11. Needs Identification			1%	14%	-1%	2%
D.12. Security Consulting			-2%	7%		8%
E.1. Forecast Development			-4%	-4%		-1%
E.2. Project and Portfolio Management		-1%	-3%	14%	1%	1%
E.3. Risk Management		21%	11%	5%		27%
E.4. Relationship Management			4%	1%		9%
E.5. Process Improvement			0%	-2%		1%
E.6. Quality Management and Compliance		16%	-2%	0%		15%
E.7. Business Change Management			1%	0%	6%	6%

E.8. Information Security Management		11%	4%	0%		19%
E.9. Information Systems Governance				0%	0%	5%

Table AJ. Gap Analysis per level (incl. Total vacancy, CyberHub, Trends, Focus Groups) for all Courses. Based on country data (Croatia, Cyprus, The Netherlands), vacancy analysis (n=606) and course offers (n=85).

6.2.3 Trainings

For training programmes, compared to education, we see a small shift in the top 20 . 'A.5. Architecture design' and 'E.8. Information Security Management' are no longer part of the top 20 gaps, and therefore the top 20 gaps can be related to eight competences. The five most important priorities for expanding the offers of training are:

1. Systems Management (C.5., Level 2)
2. Problem Management (C.4., Level 2)
3. Education and Training Provision (D.3., Level 2)
4. Systems Management (C.5., Level 1)
5. Problem Management (C.4., Level 3)

	GAP in %					
Competence/ Proficiency level	**Level e-1**	**Level e-2**	**Level e-3**	**Level e-4**	**Level e-5**	**Overall**
A.1. IS and Business Strategy Alignment				2%	1%	6%
A.2. Service Level Management			0%	0%		0%
A.3. Business Plan Development			0%	0%	-2%	0%
A.4. Product/ Service Planning		-1%	0%	0%		0%
A.5. Architecture Design			12%	4%	3%	14%
A.6. Application/ Product Design	2%	3%	0%			4%
A.7. Technology Trend Monitoring			0%	5%	-1%	9%
A.8. Sustainability Management			1%	0%		1%
A.9. Innovating				0%	-3%	0%
A.10. User Experience		-3%	1%	0%		1%
B.1. Application/ Product Development	6%	7%	6%			11%
B.2. Component Integration		0%	4%	0%		6%
B.3. Testing	17%	23%	8%	19%		25%
B.4. Solution Deployment	0%	4%	-6%			6%
B.5. Documentation Production	4%	9%	-3%			14%
B.6. ICT Systems Engineering			9%	4%		15%
C.1. User Support	0%	1%	1%			4%
C.2. Change Support		3%	-1%			4%
C.3. Service Delivery	-1%	0%	2%			2%
C.4. Problem Management		28%	26%	20%		37%
C.5. Systems Management	26%	29%	19%			34%
D.1. Information Security Strategy Development				2%	4%	13%
D.2. Quality Strategy Development				2%	0%	2%
D.3. Education and Training Provision		28%	21%			29%
D.4. Purchasing		1%	0%	0%		1%
D.5. Sales Development		0%	0%	0%		1%
D.6. Digital Marketing		0%	0%	0%		0%
D.7. Science and Analysis		12%	12%	11%	13%	19%
D.8. Contract Management		-2%	0%	0%		0%
D.9. Personnel Development		15%	15%	15%		17%
D.10. Information and Knowledge Management			1%	0%	3%	4%
D.11. Needs Identification			0%	1%	0%	3%
D.12. Security Consulting			5%	5%		13%
E.1. Forecast Development			1%	0%		1%
E.2. Project and Portfolio Management		-2%	2%	0%	-4%	2%
E.3. Risk Management		14%	12%	13%		28%
E.4. Relationship Management			10%	2%		9%
E.5. Process Improvement			3%	1%		3%
E.6. Quality Management and Compliance		14%	8%	11%		18%
E.7. Business Change Management			7%	6%	3%	7%
E.8. Information Security Management		-2%	11%	-1%		20%

E.9. Information Systems Governance				-9%	0%	4%

Table AK. Gap Analysis per level (incl. Total vacancy, CyberHub, Trends, Focus Groups) for all Trainings. Based on country data (Croatia, Cyprus, The Netherlands), vacancy analysis (n=606) and training offers (n=70).

6.3 Differences between countries

6.3.1 The Netherlands

For the Netherlands, we observe that the top 20 important gaps are related to only eight competences: 'B.3. Testing', 'C.4. Problem Management', 'C.5. Systems Management', 'D.3. Education and Training Provision', 'D.9. Personnel Development', 'E.3. Risk Management', 'E.6. Quality Management and Compliance', and 'E.8. Information Security Management' (see Table AL). The top five gaps and therefore priorities for investment are:

1. Problem Management (C.4., level 4)
2. Systems Management (C.5., level 1)
3. 3/4/5. Risk Management (E.3., remarkably, there is a large gap for levels 2, 3, and 4)

	GAP in %					
Competence/ Proficiency level	**Level e-1**	**Level e-2**	**Level e-3**	**Level e-4**	**Level e-5**	**Overall**
A.1. IS and Business Strategy Alignment				0%	2%	1%
A.2. Service Level Management			-1%	-1%		-2%
A.3. Business Plan Development			-4%	-1%	-1%	-7%
A.4. Product/ Service Planning		-7%	-3%	-1%		-11%
A.5. Architecture Design			-10%	0%	9%	-16%
A.6. Application/ Product Design	-1%	-10%	-9%			-24%
A.7. Technology Trend Monitoring			-1%	0%	3%	-1%
A.8. Sustainability Management			-2%	-1%		-2%
A.9. Innovating				-3%	0%	-3%
A.10. User Experience		-8%	-3%	-2%		-13%
B.1. Application/Product Development	3%	-1%	-16%			-29%
B.2. Component Integration		-9%	-12%	1%		-24%
B.3. Testing	13%	17%	14%	18%		1%
B.4. Solution Deployment	-6%	-4%	-7%			-18%
B.5. Documentation Production	-3%	-9%	-6%			-22%
B.6. ICT Systems Engineering			-8%	9%		-13%
C.1. User Support	-5%	-4%	-3%			-12%
C.2. Change Support		-1%	-3%			-4%
C.3. Service Delivery	-1%	0%	0%			-1%
C.4. Problem Management		19%	19%	24%		6%
C.5. Systems Management	22%	16%	14%			-5%
D.1. Information Security Strategy Development				5%	7%	6%
D.2. Quality Strategy Development				-1%	0%	-1%
D.3. Education and Training Provision		19%	19%			15%
D.4. Purchasing		-4%	0%	0%		-4%
D.5. Sales Development		-1%	-1%	0%		-1%
D.6. Digital Marketing		-1%	-1%	0%		-1%
D.7. Science and Analysis		4%	-5%	4%	13%	-23%
D.8. Contract Management		-1%	0%	0%		-1%
D.9. Personnel Development		16%	10%	17%		9%
D.10. Information and Knowledge Management			-7%	1%	3%	-9%
D.11. Needs Identification			-13%	-4%	0%	-16%
D.12. Security Consulting			-1%	-2%		-7%
E.1. Forecast Development			-4%	-1%		-5%
E.2. Project and Portfolio Management		-15%	-12%	-4%	1%	-31%
E.3. Risk Management		21%	21%	20%		14%
E.4. Relationship Management			0%	7%		0%
E.5. Process Improvement			-13%	-3%		-16%
E.6. Quality Management and Compliance		17%	9%	14%		6%
E.7. Business Change Management			2%	5%	5%	1%
E.8. Information Security Management		7%	8%	16%		-3%

E.9. Information Systems Governance		-1%	5%	-1%

Table AL. Gap Analysis per level for all education, courses and trainings based on country data the Netherlands

The most important gap, 'C.4. Problem Management', plays a vital role in ensuring the stability, security, and resilience of digital infrastructures. As Dutch organisations continue to accelerate their digital transformation, the demand for professionals with advanced competences in developing, managing, and operating ICT systems and applications has grown substantially. Within this context, problem management emerges as a key capability. This competence involves the systematic identification of root causes behind system incidents and the implementation of sustainable solutions to prevent recurrence. In cybersecurity, effective problem management is essential for mitigating risks, reducing the impact of repeated vulnerabilities, and enabling a proactive approach to threat detection and response. Consequently, it contributes not only to operational continuity but also to the strategic enhancement of organisational digital resilience.

'C.5. Systems Management' has been identified as the second most significant competence gap, a finding consistently supported by trend analyses, literature reviews, and focus group discussions. These sources collectively highlight systems management as an increasingly vital skill in the context of digital transformation and cybersecurity. As organisations become more dependent on complex and interconnected ICT infrastructures, the competence to configure, monitor, and maintain these systems securely has become essential. Systems management plays a critical role in ensuring the integrity, availability, and confidentiality of digital assets. It enables professionals to maintain oversight of system configurations, detect anomalies, and enforce security policies across diverse technological environments. This competence is particularly important in preventing misconfigurations—one of the leading causes of security breaches. Furthermore, effective systems management facilitates timely patching and updating, continuous performance monitoring, and coordinated incident response. In an era characterised by persistent and sophisticated cyber threats, the integration of systems management into cybersecurity strategies is not merely beneficial but foundational.

'E.3. Risk Management' has been identified as the third, fourth, and fifth most significant competence gap across levels e-2, e-3, and e-4, respectively. This finding is consistently supported by trend analyses, literature reviews, and focus group discussions, which emphasise the growing relevance of this competence in the cybersecurity domain. In an environment marked by rapid technological advancement and increasing exposure to cyber threats, the ability to manage risk effectively is essential for maintaining organisational resilience and ensuring the continuity of critical digital services. Cybersecurity risks are inherently multifaceted, involving technical, organisational, and human dimensions. The competence of risk management equips professionals with the necessary tools and methodologies to systematically identify, assess, and mitigate these risks. This includes conducting comprehensive risk assessments, determining appropriate mitigation strategies, and providing leadership in the development and implementation of organisational risk policies. By prioritising and allocating resources based on risk exposure, organisations can proactively address vulnerabilities and reduce the likelihood and impact of security incidents.

It is important to note that, in addition to technical competences, the vacancy analysis, focus groups and trend analyses consistently emphasise the significance of 'E.4. Relationship Management' as a foundational skill. In particular, the ability to translate complex technical risks into language that is understandable and actionable for business stakeholders is highlighted as a critical enabler of many other cybersecurity-related competences.
We also observe that the Dutch vacancies indicated five key competences as being in demand within the field of Security Consulting: 'D.1.2. Security Consulting', 'E.4. Relationship Management', 'D.7. Science and Analysis', 'B.1. Application/Product Development', and 'C.4. Problem Management'. Not all of these competences appear prominently as gaps in the data. With the exception of 'C.4. Problem Management' and 'D.7. Science and Analysis', we find that there is no significant discrepancy between demand and supply. This suggests that Dutch educational programmes are reasonably well aligned with the most sought-after skills in the labour market.

6.3.2 Greece

For Greece, we observe that the top 20 important gaps are concentrated in a compact set of Build/Plan competencies: architecture design (A.5), application/product design (A.6), application/product development (B.1), testing (B.3) and ICT systems engineering (B.6) (see Table 12). In contrast, most Enable/Manage governance items—particularly risk management (E.3), information security management (E.8) and information systems governance (E.9)—are broadly balanced or oversupplied by education/training relative to what appears in publicly advertised vacancies. The top five gaps and therefore priorities for investment are:

- Problem architecture design (A.5, level 3)
- Testing (B.3, level 3)
- Application/product design (A.6, level 3)
- Application/product development (B.1, level 3)
- ICT systems engineering (B.6, level 4)

Competence/ Proficiency level	Level e-1	Level e-2	Level e-3	Level e-4	Level e-5	Overall
A.5 Architecture Design			12.83%			12.83%
A.6 Application/ Product Design			7.34%			7.34%
A.7 Technology Trend Monitoring			−15.11%	−32.23%		
B.1 Application/ Product Development			7.34%			7.34%
B.3 Testing			8.86%			8.86%
B.6 ICT Systems Engineering				7.34%		7.34%
E.3 Risk Management			−20.47%	−38.11%		
E.8 Information Security Management			−24.73%	−43.17%		
E.9 Information Systems Governance				−8.22%		−8.22%

Table AM. Gap Analysis per level for all education, courses and trainings based on country data Greece.

Across proficiency levels, the quantitative differentials are clearest at e-3 for A.5 (largest positive delta), B.3, A.6 and B.1, and at e-4 for B.6. Conversely, several governance competences register negative deltas (supply ≥ demand): E.3 Risk Management is notably strong in supply (especially at e-3/e-4), as are E.8 Information Security Management and A.7 Technology Trend Monitoring. In practical terms, this means Greece's programmes already equip many learners for governance/ISMS/risk roles, while the mid/advanced design–build

capability required by market postings is the area where capacity expansion will yield the highest marginal benefit.

The top-five gaps for Greece remain A.5(e-3), B.3(e-3), A.6(e-3), B.1(e-3), B.6(e-4). Conversely, E.3/E.8/E.9 show negative gaps because the education/training supply covers these more broadly (and at higher levels) than what appears explicitly in 2024 public vacancy adverts. The most important gap, architecture design (A.5, level 3), is central to Greece's secure-by-design ambitions as organisations modernise platforms and migrate to cloud/data-centric architectures. At this proficiency, professionals must take regulatory and business requirements and translate them into workable security architectures, reference control sets and enforceable non-functional attributes.

Risk Assessment and Management (RA/RM) work is often embedded under consulting roles. Greek postings frequently bundle ISO 27001 RA/RM into broader D.12 Security Consulting or GRC job families rather than advertising "Risk Manager" as a standalone title. This depresses the explicit vacancy coverage for E.3/E.8 even though those competences are actually practiced inside consulting engagements. Addressing this gap accelerates consistent control selection, clarifies system boundary decisions (e.g., identity planes, network segmentation, data-at-rest/-in-use protections) and strengthens the handover from design to implementation teams.

Testing (B.3, level 3) emerges as the second most significant gap. Greek postings repeatedly call for assurance embedded in delivery—from SAST/DAST/IAST and dependency hygiene to control-validation in pipelines and environment hardening tests. Strengthening level-3 testing capability reduces misconfiguration risk, shortens remediation cycles and produces audit-ready evidence for ISMS and sectoral regimes, thereby improving mean time to detect/mend and overall delivery quality.

The third and fourth gaps—application/product design (A.6, level 3) and application/product development (B.1, level 3)—underline the need to push security left in product and platform devops. Practitioners should be able to specify secure interfaces and component contracts, apply defensive patterns, and implement security controls as code and templates across CI/CD. The fifth gap, ICT systems engineering (B.6, level 4), points to the requirement for systems-level proficiency that integrates identity, network and data protection patterns into heterogeneous estates, including hybrid/multi-cloud and containerised workloads.

It is important to note that, in addition to technical competencies, the vacancy analysis, focus groups and trend analyses consistently emphasise the significance of relationship management (E.4) as a foundational skill. The ability to acknowledge risks and design trade-offs in business terms, secure stakeholder alignment and sustain change across multiple suppliers remains a critical skill for the majority of projects in the Greek context.

We also observe that Greek vacancies indicate a stable Security Consulting cluster and an active pipeline of ISO 27001 risk assessment/risk management (RA/RM) projects. The data show D.12 Security Consulting to be well aligned (no material aggregate gap), while E.3 Risk

Management appears oversupplied in the education/training dataset at e-3/e-4. This is not contradictory: many RA/RM assignments in Greece are executed within consulting engagements, and postings frequently bundle RA/RM under broader consulting or GRC roles rather than advertising them as standalone risk positions.

- The practical implication is that the coverage gap is not in "having RA/RM at all," but in specific RA/RM proficiencies and contexts that the market increasingly needs: quantitative or semi-quantitative methods for prioritisation, third-party/supply-chain risk, cloud/shared-responsibility risk modelling, continuous / automated RA integrated with DevSecOps, and ICS/OT-specific RA aligned to NIS2/DORA and sectoral guidance. Strengthening these specialised RA/RM capabilities inside consulting curricula and apprenticeships—and coupling them tightly to architecture and testing work products—will keep Greece's strong RA/RM tradition relevant while closing the concrete design–build gaps that the 2024 vacancy data surface.

There is a clear misalignment between training supply and labour market demand in Greece. Despite some positive developments in postgraduate education and non-formal training, entry-level gaps, limited professional certification uptake, and low awareness among employers hinder effective workforce preparation. A strategic alignment between education, certifications, ECSF roles, and employer needs is essential. The most-needed skills are strictly cybersecurity-related.

6.3.3 Cyprus

For Cyprus, we observe that the top 20 most important gaps are related to 11 competences: 'A.5. Architecture Design', 'A.7. Technology Trend Monitoring', 'B.3. Testing', 'B.4. Solution Development', 'B.5. Documentation Production', 'C.4. Problem Management', 'C.5. Systems Management', 'D.3. Education and Training Provision', 'D.7. Science and Analysis', 'D.12. Security Consulting', 'E.3. Risk Management', and 'E.6. Quality Management and Compliance' (see Table AN). The top five gaps and therefore priorities for investment are:

1. Problem Management (C.4., level 3)
2. Education and Training Provision (D.3., level 2)
3. Technology Trend Monitoring (A.7., level 4)
4. Security Consulting (D.12., level 3)
5. Testing (B.3., level 2)

	GAP in %					
Competence/ Proficiency level	**Level e-1**	**Level e-2**	**Level e-3**	**Level e-4**	**Level e-5**	**Overall**
A.1. IS and Business Strategy Alignment				2%	2%	2%
A.2. Service Level Management			0%	0%		0%
A.3. Business Plan Development			2%	0%	0%	2%
A.4. Product/ Service Planning		0%	0%	0%		0%
A.5. Architecture Design			23%	13%	8%	27%
A.6. Application/ Product Design	2%	7%	2%			7%
A.7. Technology Trend Monitoring			-22%	43%	2%	20%
A.8. Sustainability Management			0%	0%		0%
A.9. Innovating				0%	0%	0%
A.10. User Experience		0%	0%	0%		0%
B.1. Application/ Product Development	-1%	9%	7%			2%

B.2. Component Integration		2%	2%	2%		2%
B.3. Testing	23%	40%	25%	21%		47%
B.4. Solution Deployment	2%	32%	0%			34%
B.5. Documentation Production	4%	36%	2%			38%
B.6. ICT Systems Engineering			0%	16%		3%
C.1. User Support	0%	5%	0%			5%
C.2. Change Support		0%	0%			0%
C.3. Service Delivery	2%	0%	0%			2%
C.4. Problem Management		35%	67%	28%		74%
C.5. Systems Management	29%	38%	29%			38%
D.1. Information Security Strategy Development				15%	6%	15%
D.2. Quality Strategy Development				0%	0%	0%
D.3. Education and Training Provision		55%	25%			57%
D.4. Purchasing		0%	0%	0%		0%
D.5. Sales Development		0%	0%	0%		0%
D.6. Digital Marketing		0%	0%	0%		0%
D.7. Science and Analysis		39%	8%	13%	13%	34%
D.8. Contract Management		0%	0%	0%		0%
D.9. Personnel Development		17%	17%	17%		17%
D.10. Information and Knowledge Management			3%	5%	3%	5%
D.11. Needs Identification			0%	0%	0%	0%
D.12. Security Consulting			41%	5%		41%
E.1. Forecast Development			0%	0%		0%
E.2. Project and Portfolio Management		0%	0%	0%	0%	0%
E.3. Risk Management		-8%	11%	24%		-21%
E.4. Relationship Management			12%	7%		12%
E.5. Process Improvement			0%	2%		2%
E.6. Quality Management and Compliance		24%	29%	17%		37%
E.7. Business Change Management			6%	6%	6%	6%
E.8. Information Security Management		12%	19%	17%		14%
E.9. Information Systems Governance				-29%	7%	-26%

Table AN. Gap Analysis per level for all education, courses and trainings based on country data Cyprus.

Overall, Cyprus shows a mixed picture of alignment. On the one hand, most competences are relatively well addressed, with only two competences appearing in persistent “red zones” (more education than demand). On the other hand, several individual gaps are particularly high, pointing to structural weaknesses. The largest gap is in ‘C.4. Problem Management’ (74%), which is critical for ensuring operational stability. This shortage may significantly affect the ability of Cypriote organisations, especially SMEs, to resolve root causes of security breaches and maintain service continuity.

The second most pressing gap is ‘D.3. Education and Training Provision’ (57%), which indicates a lack of internal capacity to prepare new cybersecurity professionals and deliver in-house training. Further high gaps are found in ‘B.3. Testing (47%), ‘B.5. Documentation Production’ (38%), and ‘C.5. Systems Management’ (38%). These areas represent essential operational competences for ensuring the reliability, maintainability, and security of ICT systems.

In conclusion, while Cyprus’s education and training landscape is broadly aligned with overall market needs, the presence of disproportionately high gaps in the abovementioned areas signals structural vulnerabilities. Addressing these should be a priority for future training investment to strengthen national resilience and internal workforce development.

6.3.4 Croatia

For Croatia, we observe that the top 20 most important gaps are related to ten competences: 'B.3. Testing', 'B.5. Documentation Production', 'C.1. User Support', 'C.4. Problem Management', 'C.5. Systems Management', 'D.1. Information Security Strategy Development', 'D.3. Education and Training Provision', 'D.9. Personnel Development', 'E.3. Risk Management', 'E.6. Quality Management and Compliance', and 'E.8. Information Security Management' (see Table AO). The top five gaps and therefore priorities for investment are:

1. Problem Management (C.4., level 3)
2. Education and Training Provision (D.3., level 2)
3. Risk Management (E.3., level 3)
4. Information Security Strategy Development (D.1., level 4)
5. Education and Training Provision (D.3., level 3)

	GAP in %					
Competence/ Proficiency level	**Level e-1**	**Level e-2**	**Level e-3**	**Level e-4**	**Level e-5**	**Overall**
A.1. IS and Business Strategy Alignment				10%	2%	10%
A.2. Service Level Management			0%	0%		0%
A.3. Business Plan Development			-5%	-1%	-1%	-7%
A.4. Product/ Service Planning		-11%	-2%	-1%		-14%
A.5. Architecture Design			-12%	0%	12%	-17%
A.6. Application/ Product Design	-3%	-15%	-17%			-40%
A.7. Technology Trend Monitoring			1%	-1%	3%	-1%
A.8. Sustainability Management			-4%	-1%		-5%
A.9. Innovating				-5%	0%	-5%
A.10. User Experience		-11%	-8%	-3%		-22%
B.1. Application/ Product Development	5%	-3%	-31%			-43%
B.2. Component Integration		-10%	-15%	8%		-20%
B.3. Testing	9%	26%	8%	14%		-5%
B.4. Solution Deployment	-10%	-3%	-8%			-20%
B.5. Documentation Production	13%	18%	-8%			18%
B.6. ICT Systems Engineering			-18%	14%		-18%
C.1. User Support	-5%	15%	1%			11%
C.2. Change Support		12%	2%			14%
C.3. Service Delivery	-1%	3%	3%			4%
C.4. Problem Management		24%	39%	18%		25%
C.5. Systems Management	20%	21%	7%			-9%
D.1. Information Security Strategy Development				33%	11%	38%
D.2. Quality Strategy Development				3%	2%	5%
D.3. Education and Training Provision		35%	30%			42%
D.4. Purchasing		1%	2%	0%		3%
D.5. Sales Development		1%	3%	0%		4%
D.6. Digital Marketing		-1%	-1%	1%		-1%
D.7. Science and Analysis		5%	-19%	-4%	13%	-45%
D.8. Contract Management		3%	2%	0%		5%
D.9. Personnel Development		16%	10%	17%		9%
D.10. Information and Knowledge Management			3%	1%	3%	1%
D.11. Needs Identification			-13%	-2%	0%	-15%
D.12. Security Consulting			10%	11%		16%
E.1. Forecast Development			-5%	-2%		-7%
E.2. Project and Portfolio Management		-20%	-7%	-4%	1%	-30%
E.3. Risk Management		24%	33%	20%		29%
E.4. Relationship Management			-2%	6%		-3%
E.5. Process Improvement			-13%	-7%		-20%
E.6. Quality Management and Compliance		15%	-1%	11%		-10%
E.7. Business Change Management			-3%	6%	6%	-3%
E.8. Information Security Management		-1%	14%	15%		-6%
E.9. Information Systems Governance				-6%	5%	-6%

Table AO. Gap Analysis per level for all education, courses and trainings based on country data Croatia.

The following important country specific conclusions can be made:

- **Technical vs. strategic skill production**: Croatian cybersecurity education programmes are producing an abundance of technically skilled practitioners (e.g., developers, testers, analysts) in excess of what the current market explicitly demands. For instance, over 60% of courses teach programming and development (B.1.), whereas only 13% of security jobs require that competence. Meanwhile, strategic and management skills are in shortage – only ~1 in 11 programmes addresses information security strategy (D.1.), yet 2 in 5 job postings require it. This imbalance suggests a workforce pipeline that is heavy on entry-level and mid-level technical skills but thin at the top, where strategic leadership is needed.
- **Implications of gaps**: The observed gaps portend potential shortages in filling senior cybersecurity roles. Notably, roles such as CISO, Security Manager, or Cybersecurity Auditor can be challenging to staff with local talent, as few training programmes cultivate the full spectrum of competences these jobs require. For example, a CISO position typically requires aligning security with business strategy (A.1.) and developing comprehensive security strategies (D.1.); yet, these are among the least-covered skills in curricula. Similarly, a Cybersecurity Auditor or Compliance Officer would benefit from training in quality strategy (D.2.) in addition to compliance; however, virtually no courses teach how to develop quality and security improvement strategies. The risk is that graduates may enter the workforce well-versed in tools and technologies but lack the high-level perspective, risk management finesse, and policy and strategy experience to assume leadership roles. Employers may struggle to find suitable candidates for senior openings domestically, potentially leading to unfilled positions or a reliance on external hires or expatriates. On the other hand, the oversupply of technical skills could mean that junior professionals face greater competition for roles, or they may need to upskill in soft and strategic areas on the job to advance.
- **Recommendations – Targeted training expansion**: To better align with market needs, it is recommended that training providers expand and diversify their cybersecurity curricula in specific areas. In particular, strategic planning and governance topics should be bolstered. Universities and academies could introduce advanced modules on '*D.1. Information Security Strategy Development'* and *'A.1. Business-IT Strategy Alignment'*, perhaps via case studies and capstone projects that simulate CISO decision-making, given that these are demanded by ~40% and 17% of employers, respectively. 'E.3. Risk Management' content can be maintained or enhanced, ensuring students can progress to level e-5 proficiency, since demand for high-level risk skills remains robust (over one-third of jobs). Programmes should also integrate leadership and consulting skills practice – for example, offering coursework or workshops on *'D.12. Security Consulting'*, client communication, and security program auditing. That could help address the ga. Additionally, increasing coverage of *'D.3. Education & Training Provision'* – e.g. by having students conduct security awareness sessions or mentorship as part of their training. Technical versus Strategic Skill Development: Croatian cybersecurity education programmes are generating a surplus of technically proficient practitioners (e.g., developers, testers, analysts) beyond the explicit expectations of the existing market. For example, more than 60% of courses instruct on programming and development (B.1.), but merely 13% of security positions require that skill. Currently, strategic and management abilities are deficient; approximately 1 in 11 programmes covers information security strategy (D.1.), whereas 40% of job listings necessitate it. This disparity

indicates a personnel pipeline that is abundant in entry-level and mid-level technical competences but deficient at the upper echelons, where strategic leadership is essential.

- **Consequences of discrepancies**: The identified gaps indicate possible deficits in fulfilling senior cybersecurity positions. Positions such as CISO, Security Manager, or Cybersecurity Auditor may be challenging to fill with local talent due to the scarcity of training programmes that develop the comprehensive skill set required for these roles. The CISO role generally necessitates aligning security with corporate strategy (A.1.) and formulating comprehensive security strategies (D.1.); nevertheless, these competences are among the least addressed in educational curricula. A Cybersecurity Auditor or Compliance Officer would similarly benefit from training in quality strategy (D.2.) alongside compliance; yet, there are almost no courses that instruct on the development of quality/security improvement strategies. The concern is that graduates may possess proficiency in tools and technology, yet lack the strategic insight, risk management acumen, and policy and strategy experience necessary for leadership positions. Employers may encounter difficulties in locating suitable candidates for senior jobs locally, potentially resulting in unfilled roles or a reliance on external hiring or expatriates. Conversely, the surplus of technical abilities may result in increased rivalry for junior professionals seeking positions, necessitating the enhancement of soft and strategic competences in the workplace to progress.
- **Recommendations – Focused training enhancement**: Training providers should enhance and broaden their cybersecurity curricula in targeted areas to better correspond with market demands. Specifically, strategic planning and governance issues should be enhanced. Universities and academies could implement advanced modules on ‘D.1. Information Security Strategy Development’ and ‘A.1. Business-IT Strategy Alignment’, potentially through case studies and capstone projects that replicate CISO decision-making, as these are sought by approximately 40% and 17% of employers, respectively. ‘E.3. Risk Management’ curriculum can be preserved or improved, facilitating students' advancement to level e-5 proficiency, as the need for advanced risk skills remains strong (exceeding one-third of employment opportunities). Programmes should incorporate the practice of leadership and consulting skills, such as providing coursework or seminars on ‘D.12. Security Consulting’, client communication, and security program audits. Furthermore, enhancing the scope of ‘D.3. Education & Training Provision’ – for instance, by incorporating student-led security awareness sessions or mentorship into their training – would equip future leaders to undertake one-third of cybersecurity positions that entail training or coaching duties.

According to expert analysis, it is essential for Croatian cybersecurity training programmes to deliberately incorporate lessons on secure software development, binary analysis, and malware reverse engineering, particularly as the complexity of cyber threats continues to increase. These subjects are crucial for Security Operations Centre (SOC)/CERT teams, defenders of vital infrastructure, and advanced red and blue teams, as well as for establishing national cyber resilience. Their exclusion from conventional frameworks should not be misconstrued as an absence of necessity; instead, they ought to be regarded as interdisciplinary specialisations that enhance both operational and strategic cybersecurity functions.

The gap analysis indicates that Croatia's cybersecurity education framework possesses robust foundations in technical skill training but requires advancement to foster higher-level competences. By adjusting the curriculum to incorporate additional strategic, risk management, leadership, and consulting components (while maintaining essential technical skills), training providers can guarantee that graduates fulfil current market demands and are prepared to evolve into the next generation of Chief Information Security Officers, security consultants, and auditors. This focused upskilling will address the highlighted deficiencies, ultimately alleviating talent shortages at senior levels and aligning educational achievements with the demands of the cybersecurity job market.

7 PRACTICAL USES & VISUALISATION

7.1 Functional & technical requirements CYTIM

The **CADMUS project's mission** is to address the cybersecurity skills shortage in Europe by developing targeted trainings and aligning them with industry needs (CADMUS, 2025b). A foundational step in this mission is to survey and map what training is already out there – this is exactly what the Cybersecurity Training Initiatives Map (CYTIM) accomplishes. The data collected in CYTIM serves as the empirical basis for understanding the current landscape of cybersecurity education and training:

- **It captures the status quo**. By listing existing initiatives, CADMUS can avoid duplicating existing offerings and instead identify where new programmes are needed. For instance, if CYTIM shows many ethical hacking courses but few defensive security architecture courses, the project might decide to develop training in the latter area.
- **It facilitates skills gap analysis**. CYTIM doesn't just list courses, it evaluates them against the needed skill sets (via role and competence coverage). This directly supports the WP2 objective of detecting skills gaps (CADMUS, 2025c). The mapping can highlight gaps both geographically (gaps in certain countries or regions) and topically (gaps in coverage of certain roles or skills). For example, CADMUS evaluators can query how many courses in Europe cover the "Cybersecurity Risk Manager" role or teach 'E.3. Risk Management' competence; if the numbers are low, that indicates a gap to address.
- **It provides a resource for stakeholders**. CYTIM is also a dissemination tool under WP6 (Dissemination and Communication) to "promote cybersecurity training opportunities across Europe" (CADMUS, 2025c). By publishing this mapping on a web platform, CADMUS makes it easier for individuals (students, IT professionals) and organisations (SMEs, public sector bodies) to find relevant training opportunities. In other words, it's not just an internal analysis tool, but also an outward-facing service to connect people with training, thereby helping to **bridge the cybersecurity skills gap** with better information. The European Commission's focus is on bringing together initiatives (as seen with the Cybersecurity Skills Academy) and improving coordination (ENISA, 2022a); CYTIM contributes to this by aggregating training info in one place.
- **It creates a baseline for further expansion**. The current data is a starting point. The plan would be to expand the database to more EU countries and keep it updated. The structure is in place to incorporate new entries seamlessly (thanks to the standardised format). As CADMUS progresses (the project runs for 36 months from late 2024, CADMUS, 2025b), one can expect CYTIM to grow into a comprehensive map of Europe's cybersecurity education ecosystem.

7.1.1 Rationale for implementing CYTIM as a web application

The Cybersecurity Training Initiatives Map (CYTIM) is positioned to serve a broad set of stakeholders across the European cybersecurity education and labour-market ecosystem. At policy level, EU institutions and agencies can use CYTIM to monitor whether funded skills initiatives under the Cybersecurity Skills Academy are materialising into training supply that

aligns with identified workforce needs. They can interrogate coverage against the European Cybersecurity Skills Framework (ECSF) roles and associated e-Competences and proficiency levels (e-1 to e-5), and then route funding or calls to correct imbalances at EU or cross-border level. National ministries, cybersecurity authorities and Digital/Skills agencies can use CYTIM to plan or co-finance national programmes. A ministry can, for example, assess whether domestic offers mapped to the "Cyber Incident Responder" or "Cybersecurity Risk Manager" roles exist at e-4/e-5 proficiency and whether they are reachable outside capital regions. Higher education institutions, VET providers and private training companies are direct beneficiaries. They can benchmark their portfolios against ECSF roles and e-Competences to discover underserved niches, while they can also use CYTIM as a dissemination channel, increasing programme visibility to learners and employers while contributing structured metadata that improves comparability across Europe. Employers, HR leaders and CISOs in SMEs and public administrations can consult CYTIM to source training aligned to specific work roles and proficiency needs rather than generic course titles, and career services, employment offices, and re-skilling programmes can use CYTIM for personalised guidance.

What becomes apparent is that many user groups share overlapping or similar tasks, resulting in a corresponding overlap in the types of visualisations that may be useful to them. These commonalities should be prioritised when determining which visual elements to include in the overview displays. Recurring tasks among these groups include monitoring market trends, aligning, retraining or upskilling employees and professionals, recruiting and networking, as well as integrating industry needs into educational curricula. Below, several examples of similar visualisations are presented, each of which is also referenced in the table, to serve as inspiration for future research and development.

Transitioning the CYTIM from static content formats, such as Excel files, to a dynamic JavaScript-based web application significantly enhances its accessibility, interactivity, and overall effectiveness. Unlike Excel files, which are inherently limited in usability and require manual data navigation, a web application allows for intuitive interaction through visual elements such as interactive statistics, real-time filtering, and dynamic updates.

Utilising JavaScript enables responsive and real-time user interactions, critical for exploring complex datasets that map cybersecurity competences and roles. Interactive elements, such as clickable ECSF roles able to combine into groups, filtering by role or competency, and immediate data visualisation, significantly improve user experience, making it easier for stakeholders to derive actionable insights without needing technical knowledge of data manipulation tools.

Furthermore, a JavaScript-driven web application is highly scalable and can efficiently accommodate updates and expansions, including new training initiatives or additional countries. Updating Excel sheets require manual intervention and distribution, whereas a web application streamlines this process through automated data updates via backend APIs or JSON integrations, ensuring stakeholders always access current information.

Finally, web-based platforms enhance collaboration and dissemination, aligning with the CADMUS project's EU-wide objectives. Stakeholders across Europe can effortlessly access and engage with the content through any standard web browser, thus maximising reach and impact. In conclusion, the choice of JavaScript-based web applications over static content files substantially improves the usability, scalability, and dissemination potential, making it the superior option for implementing CYTIM.

7.1.2 Alignment with e-CF and ECSF frameworks

A key strength of the CYTIM web application is its alignment with established European frameworks for skills and roles in cybersecurity, namely the e-CF and the ECSF. This alignment ensures that the tool's outputs are relevant and immediately applicable to European policy goals and industry needs. It elevates the conversation from "course A vs course B" to "which competences and roles are we strengthening, and which need more attention?" which is exactly the perspective needed to systematically close the cybersecurity skills gap in Europe.
CYTIM leverages the e-CF and ECSF frameworks by mapping each training initiative in its database to the relevant ECSF roles and e-CF competences. A user (or policymaker) can thus see which competences (in e-CF terms) and which job profiles (in ECSF terms) are addressed by current training offerings, facilitating comparisons and gap analysis across initiatives.

Furthermore, CYTIM's alignment efforts extend to collaborating with international training and certification providers to integrate their offerings under the ECSF/e-CF schema. Many globally recognised cybersecurity certifications have been mapped to the e-CF and/or ECSF roles by their issuing bodies or others, and CYTIM takes advantage of these mappings. The project team engaged with leading certification organisations (such as (ISC), ISACA, CompTIA, SANS, CREST and others) to include their certification programmes in the initiatives map. By doing so, the platform incorporates data on certifications like CISSP, CISM, CompTIA Security+, Global Information Assurance Certification (GIAC) certifications, etc., and shows how these credentials correspond to the European skill framework. Indeed, several major certification bodies have already aligned their credential portfolios with the ECSF's role profiles (ENISA, 2022d). CYTIM builds on this by integrating those certifications and denoting, for example, which ECSF roles each certification most directly supports. This collaboration ensures that the taxonomy is comprehensive and internationally relevant – the mapping does not only cover academic courses or national programmes, but also industry certifications that are key to cybersecurity careers. In summary, CYTIM is a knowledge base whose content and structure mirror the ECSF and e-CF frameworks. This alignment guarantees that stakeholders using CYTIM (learners, employers, educators, policymakers) can navigate training options through a familiar, standardised lens and easily cross-reference the initiatives against European-defined roles and competences.

The CYTIM web application explicitly integrates these frameworks into its data model and user interface, yielding several benefits:

- **Mapping Training to Role Profiles (ECSF):** As described earlier, each training initiative entry in CYTIM lists one or more of the 12 ECSF role profiles that the course is relevant to, along with a percentage coverage. By doing so, CYTIM makes it clear which roles a learner could

pursue after completing the training. It also allows filtering by role, meaning a user can ask "show me trainings for Digital Forensics Investigator" and the tool will respond with those that map to that role. This alignment is critical: it ensures that the data is not just a list of course titles, but is contextualised in terms of workforce needs. A policymaker can see, for instance, how many CISO-oriented programmes exist in each country, directly from the map.

- **Mapping Training to Competences (e-CF):** Each entry's list of e-CF competences (with proficiency levels) shows what skill areas are taught in that training. The website can use this mapping to enable advanced search (e.g., find all courses teaching "Risk Management"), or to display the breadth of a programme. For example, a Master's programme might cover 10 competences across technical and managerial areas, whereas a short certification course might cover 3 very specific competences. This helps users pick courses that match the skills they want to gain, and helps organisations ensure the courses cover the competences they require employees to have.
- **Ensuring Standardised Comparison:** By using e-CF and ECSF as the backbone, CYTIM allows apples-to-apples comparisons of training content. Without such frameworks, one course might say "teaches network security" and another "covers ISO 27001" – which are hard to compare. With e-CF competences, both might map to, say, 'D.1. Information Security Strategy Development'; or 'D.4. Purchasing' etc., making it evident if they overlap or differ. Similarly, role mapping avoids confusion of job titles – for example, one programme might call itself "Cybersecurity Management Training" and another "CISO Bootcamp"; mapping both to CISO role confirms they target similar outcomes.
- **User Trust and Guidance:** From an end-user perspective (say a young professional who wants to enter cybersecurity), these frameworks might not be familiar initially. However, CYTIM's use of them can introduce and guide users to think in terms of roles and competences. For instance, a user might not know what career to pursue – browsing CYTIM, they see these defined roles and what training leads to them, effectively educating the user about the cybersecurity career landscape. The site, by reflecting the ECSF roles, indirectly educates visitors on the current 12 role categories and their scope. Similarly, seeing e-CF competences listed could spark interest in understanding those competences – CYTIM could even link to definitions (perhaps via tooltips or a help section). Thus, the site becomes a learning resource about the frameworks themselves, not only a beneficiary of them.
- **Framework Evolution:** Should the frameworks update (e.g., a new version of e-CF or an extension of ECSF), the data model can accommodate that by adding new roles or competences. CYTIM could thus serve as a living example of framework adoption. It also sets a precedent; other projects or institutions might emulate this approach of tagging courses with ECSF/e-CF, and CYTIM could potentially federate or share data with other platforms like the European Cybersecurity Skills Atlas if one is created under the Skills Academy initiative.

In the User Interface (UI), this alignment is visible in multiple ways:

- Filter options by role/competence (the filter labels correspond to ECSF roles or e-CF codes).
- Display of role coverage (percentages next to standardised role names).
- Listing of competences (using the e-CF codes and names, perhaps with level indications).

The semi-formal tone of CYTIM's reporting and site content assumes users can grasp these acronyms, but it also provides full names and possibly links to more info (for example, an "About" section might explain what ECSF and e-CF are, like how we did above, to ensure all users understand why those are there).

7.1.3 Dataset structure & content

The CYTIM data structure is carefully designed to serve the dual purpose of cataloguing training initiatives and aligning them with recognised skill frameworks. Each entry is rich in information, from basic details to advanced mappings, enabling the web application to present information in a meaningful way for users and to support the CADMUS project's strategic analyses. The following sections will describe how this data is leveraged in the web application's architecture and user interface, and how the design ensures that the information is presented in an accessible, user-centred manner.

Countries as Cybersecurity Training Mapping Facets.
CYTIM mapping is underpinned by a structured dataset of cybersecurity training initiatives. Each entry in the dataset represents a distinct education, course or training programme related to cybersecurity skills development. The data is currently provided in two formats (a JSON file and an Excel sheet) and covers four countries (Croatia, Cyprus, Greece, Netherlands). In total, 266 initiatives are catalogued, encompassing both formal education programmes and shorter professional courses and trainings. This section examines the type and structure of the data loaded by the tool, explaining what each entry contains, what information is shown for each country, and how this data serves the CADMUS project's objective of mapping European cybersecurity training initiatives.

For each country, the tool presents the initiatives relevant to that country in listings. The language of instruction can be used as a filter. Many of the education programmes are collaborations with international universities (for example, some private colleges in Athens run MSc programmes in cooperation with UK universities), which is noted in the provider field.

Within a selected country, users can see the list of all initiatives for that country, possibly with an overview of types. For instance, Greece would list all 47, possibly grouped by category or city. The interface might provide a quick statistic like "Greece – 47 initiatives (21 Education programmes, 26 Courses)". Similarly, Netherlands would show "148 initiatives".

Entries as Cybersecurity Training Initiatives.
Each data entry corresponds to a cybersecurity training initiative – for example, a university master's degree programme, a certification course, a seminar, or a training bootcamp. The entries have a rich set of fields describing key attributes of the initiative. In the JSON data structure, each entry is a JSON object with fields such as those mentioned in Annex 5 Manual education initiatives Excel sheet format. Each entry, therefore, provides a comprehensive profile of a training initiative, combining general descriptors (title, provider, location) with specifics on format and content. For example, the first entry in the dataset is titled "Information Systems

Development and Security", offered by the Department of Informatics at Athens University of Economics and Business in Athens, Greece. It is categorised as an Education (postgraduate programme), delivered in a Hybrid format, conducted in Greek, with a duration of 1.5 years and an estimated workload of 40 hours per week (or a certain credit load). The description (in Greek) outlines the programme's focus on intelligent information systems and cybersecurity, its updated curriculum, and its aim to train specialised scientists with both theoretical and practical knowledge. A URL is provided for the programme's webpage. This example illustrates how an entry encapsulates key information someone might want to know when searching for cybersecurity training in a given country.

It's worth noting that the content of descriptions remains in the original language of the offering, which is appropriate for local trainees but may require translation for international users. This is a detail that might be addressed in future tool enhancements for accessibility (e.g., providing summaries in English).

Role Coverage and Competence Mapping in Each Entry.
Beyond the basic descriptors, a standout feature of the CYTIM data is the mapping of each training initiative to standard cybersecurity roles and competences. Each entry includes:

- **Relevant Cybersecurity Roles** – a list of job role profiles (drawn from the ECSF – see section 4) that the training prepares for or is relevant to. In the data, roles are given by title, for example: Chief Information Security Officer (CISO), Cyber Incident Responder, Penetration Tester, Cybersecurity Risk Manager, Digital Forensics Investigator, Cybersecurity Auditor, Cybersecurity Architect, Cyber, Legal, Policy & Compliance Officer, Cybersecurity Educator, Cybersecurity Researcher, Cybersecurity Implementer, etc.
- **Role Coverage Percentages** – for each role listed, a percentage value indicating how fully the training covers the knowledge and skill requirements of that role. A value of "100%" means the course is specifically designed to fulfil that role's competency needs completely (for example, a course on penetration testing might have Penetration Tester: 100%). Lower percentages (e.g. 40%, 20%) indicate the training covers only part of that role's scope. If a role is not relevant at all, it might either be omitted from the list or explicitly marked as 0%. In the Excel data, each role had a column, and entries contain values like "100%", "50%", "25%", or "0%" for each role. For example, the Information Systems Development and Security MSc programme in Athens is mapped to several roles: CISO (100%), Cyber Legal/Policy Officer (100%), Cybersecurity Researcher (100%), Cybersecurity Risk Manager (50%), Cyber Threat Intelligence Specialist (40%), Cybersecurity Auditor (40%), Cybersecurity Educator (~33%). Roles not applicable to that programme are 0%. These percentages provide a quantitative alignment of the training's content to job profiles – a unique aspect that helps identify how well a programme prepares for certain professional roles.
- **e-CF Competences** – a list of ICT competences from the e-CF that the training covers, along with the proficiency level(s) addressed. Competences are identified by their e-CF code (such as 'A.1. Information Systems and Business Strategy Alignment', 'D.10. Information and Knowledge Management', 'E.3. Risk Management', etc.) and the names are provided for clarity. Each competence may have one or two proficiency levels (denoted as e-1 through e-

5) associated with the training. For instance, if a course teaches risk management at an advanced level, it might list 'E.3. Risk Management – level e-4'. Some trainings span multiple proficiency levels of competence; for example, a broad programme might cover 'A.7. Technology Trend Monitoring. at both e-4 and e-5 levels. In the dataset, no competence was linked to more than two proficiency levels for a given course (reflecting that courses tend to focus within a limited range of expertise). The e-CF mapping essentially tells users what specific skills and knowledge areas (in a standardised taxonomy) the training imparts, and at what level of mastery.

7.1.4 Architecture

The CYTIM web application is built to visually and interactively represent the data described above. Its architecture can be understood in terms of a front-end interface that displays information (as an interactive mapping and associated panels) and a data layer that feeds this information (the JSON/Excel data). In this section, we describe the site's architecture and data categories, and how information is organised for the user.

The CYTIM application appears to be a client-side web tool (accessible via a URL) that uses modern web technologies (HTML5/JavaScript) to render a list-based visualisation. The architecture can be outlined as follows:

- **Front-End Interface:** The user interacts with a web page that includes a mapping of European Member States and UI controls (filters, buttons, menus). The selector is a central element, showing countries and roles. When a user selects a country, or selects filters, the displayed information updates. The interface includes a panel to list the initiatives for a selected country or to show details of a selected training.
- **Data Source:** The application loads the training data (the JSON file) in the background. Given that the data is static (at least per release), it is embedded when the page loads. Since the provided data was given in JSON, the web app directly consumes a JSON. This JSON contains all entries and is stored on the server or as a static file that the front-end code can parse. The original Excel files used were just for internal use or population of the web tool database; the live app uses JSON for performance. No back-end database or dynamic querying from server seems necessary at this stage, as the entire dataset is reasonably sized to be handled in the browser.
- **Data Categories:** The data is organised by country. The web app first presents data at the country level. Then, upon drilling down (selecting a country), it shows the list of initiatives in that country. Within each country, entries can be grouped by type (Education vs Course) or other categories like role or type of course provided (Class, Hybrid etc.).
- **Visualisation Components:**
    - **Panel**: Upon selecting a country, the interface panel allows further filtering by listing all filters that can be applied in that country. Each initiative entry in the list might be shown with key info: title, provider, icons or tags for type and delivery mode (online/hybrid), and indicators of which roles it covers. The user could click on a specific initiative in the list to expand more details (e.g., full description, link to provider site, and a breakdown of role coverage).
    - **Filters**: above or alongside the list, there are interactive filters. These could include:

- A dropdown or checklist for **Role** – allowing the user to filter initiatives by one or multiple cybersecurity role profiles (e.g., show only trainings that prepare for *Penetration Tester* or *CISO*).
- A dropdown or checklist for **Competence** – enabling filtering by e-CF competence (e.g., find all trainings that teach *"Risk Management (E.3)"*).
- Filters for **Type** – toggles or checkboxes for Education vs Course, so the user can, for instance, view only university programs or only short courses.
- Possibly a filter for **Delivery Mode** – if a user wants only Online courses, they could filter out in-person ones.
- A **search bar** for keywords – allowing text search in titles/descriptions (for example, typing "network" might filter to courses with "Network Security" in the title or content).
- Filter by **Country** – although the mapping itself is the country filter, there might also be a dropdown to jump directly to a country or compare across multiple countries (in future when many are included).

The architecture thus follows a client-side filtering model: all data is loaded, and the UI elements control which subset of data is displayed. This ensures snappy interactivity (no need to query a server for each filter change) and a cohesive single-page experience.

Figure 9. Filtering cybersecurity training programmes by Country

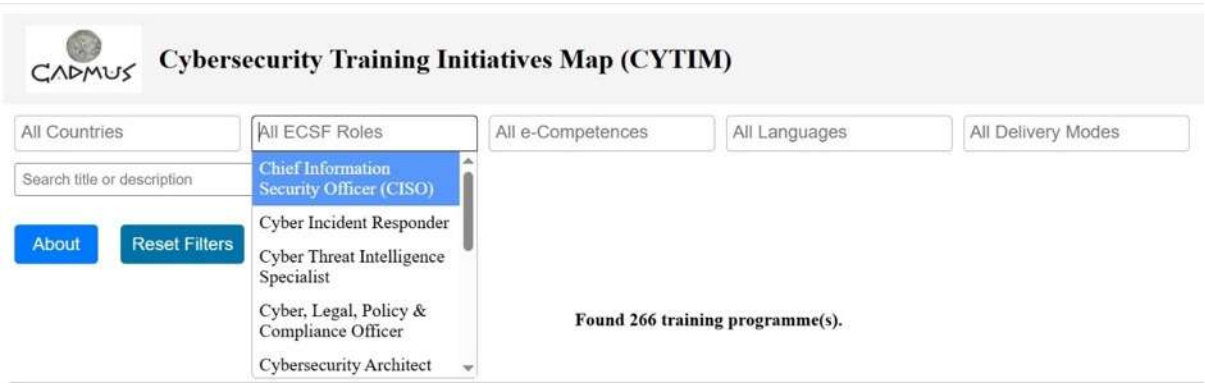

Figure 10. Filtering cybersecurity training programmes by Role

Figure 11. Filtering cybersecurity training programmes by Delivery Mode.

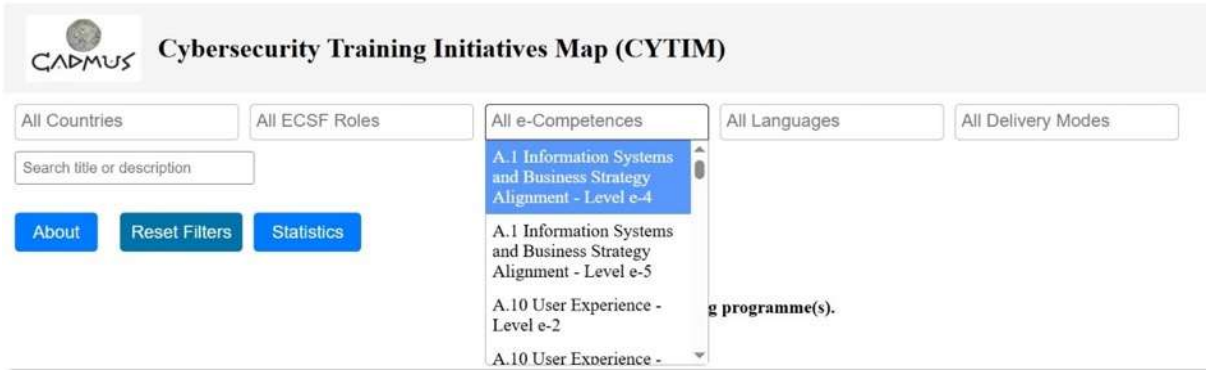

Figure 12. Filtering cybersecurity training programmes by Competence.

7.1.5 Visual and Interactive Representation of Information

The information from each initiative is presented in a way to maximize clarity and intuitiveness. The design leverages familiar visual cues and interactive elements to help users navigate the data:

- **Listing and Details:** Upon selecting a country, the list of initiatives is presented in a structured list or table. **Content organization** here is important: each entry might display a **title** (possibly clickable to expand or to open the URL in a new tab), the **provider** and location (city), and a set of icons or badges representing key attributes:
  - An icon or abbreviation for Education vs Course.
  - An icon for delivery mode (e.g., a computer screen icon for Online, a building for Classroom, etc.).
  - Possibly flags or language codes to denote the language of instruction (though if by country, users might assume the local language unless specified otherwise).

  The list might be sortable or searchable. For example, a user could sort the list alphabetically, or by type. However, since filtering is the main method, sorting might be less critical.
- **Interactive Filtering:** The filtering system is a major interactive feature. In line with UCD best practices, filters should be easy to use and understand. implementations:

- **Multi-select filters** with clearly labeled options. For example, a sidebar could list all 12 roles with checkboxes. If a user checks *Penetration Tester* and *CISO*, the list updates to show only initiatives where those roles have a non-zero coverage. The interface might highlight the filter criteria currently active (e.g., "Filtering by role: Penetration Tester, CISO").
- **Real-time feedback:** As soon as a filter is applied, results update immediately (without page reload). The number of initiatives found could be shown ("Showing 10 initiatives out of 94").
- **Combination of filters:** Users can apply multiple filters at once (e.g., Country = Greece, Role = CISO, Delivery = Online) to narrow down to, say, "online courses in Greece for CISO role". The architecture should handle these combinations, displaying "no results" message if none match.
- **Clear filter controls:** There would be an obvious way to reset filters (like an "X" or "Clear All" button) to get back to the full view.
- The design also includes a search bar for free text. This complements structured filters by allowing searches for specific terms (like "forensics" or "Master"). A user-centred approach means accommodating both users who prefer structured drill-down and those who prefer direct search.

- **Responsive Design:** Considering accessibility and usability, the site uses a responsive design to work on various screen sizes. On smaller screens, the mapping might simplify or the list might stack under the panel filters. Buttons and touch targets should be large enough for tablet use. Ensuring that the interface remains navigable on mobile would widen the accessibility, although the data-heavy nature might make it more naturally a desktop web app. Still, basic responsiveness is a UCD best practice.
- **Statistics view**: The statistics view accepts multiple role and competence parameters in the URL, for example a query combining "Cyber Incident Responder" and "Cyber, Legal, Policy & Compliance Officer" roles with "A.1 Information Systems and Business Strategy Alignment – Level e-5" and "A.4 Product/Service Planning – Level e-4". This deep-link design demonstrates multi-select filtering and shareable, reproducible queries, which are essential for collaboration among evaluators and policy teams. In practice, this pattern supports session-independent navigation, lets stakeholders embed pre-filtered snapshots in reports, and enables auditability because a chart or table can always be traced back to its exact parameter set. The query structure itself is explicit and consistent with the ECSF/e-CF vocabulary and levels, indicating that the user interface and the data model are aligned to recognised European standards. Where the catalogue page is concerned, a coherent user experience typically couples text search with faceted filters—country/region, delivery mode, language, duration, level, credential—and provides detail statistics with stable identifiers, canonical provider links and a concise mapping to roles and competences. These elements together support both exploration and precise retrieval while preserving the context that evaluators need to validate entries.

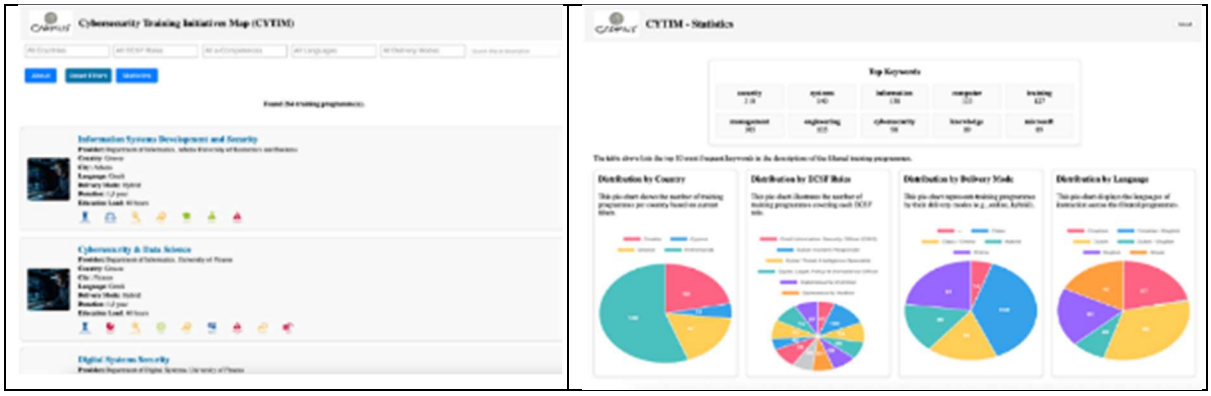

Figure 13. Visualization of CYTIM, showing the educational items with filters and the statistics page.

7.1.6 Application of UCD Principles

This section describes how User-Centred Design (UCD) principles have been (or can be) applied in the development of the tool – addressing usability, accessibility, content organisation, and interactive filtering.

The CYTIM web application's data visualisation was developed using a UCD approach, emphasising iterative refinement with continual end-user involvement (Interaction Design Foundation, 2025). In practice, the development team engaged representative users (e.g. cybersecurity professionals, learners) in multiple design-and-test cycles. Early interface prototypes were presented to these end users for feedback, and insights from usability testing were used to guide successive design improvements (Interaction Design Foundation, 2025). This iterative cycle ensured that the visualisation interface closely met user needs and expectations. Users effectively acted as an "early-warning system" to spot usability or comprehension issues that designers might overlook, allowing the team to course-correct and fine-tune the design for clarity and ease of use (Interaction Design Foundation, 2025). As a result, the final data visualisation module features intuitive navigation and interaction patterns that reflect actual user preferences discovered during the UCD process. After these iterative evaluations, the refined design was implemented in the CYTIM web application, ensuring that the interface elements and interactive charts function as validated by users during testing. Importantly, accessibility was built into this UCD process to make the visualisation module inclusive. The design team followed web accessibility best practices and conducted formal accessibility evaluations on the module's user interface. This included verifying compliance with the Web Content Accessibility Guidelines (WCAG 2.1) for things like colour contrast, keyboard navigation, and screen-reader compatibility. For example, the interface uses a colour palette and chart styles that meet recommended contrast ratios (WCAG 2.1 advises at least a 3:1 contrast for graphical elements) (HighCharts, 2022) to assist users with low vision or colour blindness. Key data insights presented in charts are also provided with text alternatives (e.g. summaries or data tables) so that users relying on assistive technologies can still obtain the information. The module was tested with tools and user feedback to ensure that all interactive features (filters, graphs) are operable via keyboard and have appropriate alternative text or

Accessible Rich Internet Applications (ARIA) labels for screen readers. By integrating these checks, the CYTIM visualisation interface meets high standards of usability and accessibility.

The site also adheres to common usability heuristics:

- **Consistency:** Visual elements like how filters behave, are consistent throughout. If, for instance, clicking Greece updates the list in real-time and re-aligns programmes, then clicking Netherlands should do the same – the user learns the interaction once and can apply it elsewhere. If courses are colour-coded (say Education programmes in one colour, short courses in another in the list), that colour coding is used uniformly.
- **Feedback:** The interface provides immediate feedback on actions. For example, selecting a country might highlight it in the choice box and show a tooltip icon (feedback that it's interactive). Clicking a filter highlights filter selection and updates the results count. Loading indicators appear if data is being fetched. If the user clicks a link to an external site (course URL), it opens a new tab, with a small icon indicating an external link.
- **Error prevention and recovery:** While the app is mostly for exploration (not data entry), a UCD approach ensures that even states like "no results found" are handled gracefully with a clear message ("No training initiatives match your filters.") rather than leaving the user staring at a blank page.

In conclusion, the website's architecture uses a country-driven, filter-supported interface to organise and present the data in an intuitive way. By adhering to UCD principles—ensuring the site is easy to navigate, information is logically structured, and features like filtering are designed around user goals—the CYTIM tool strives to be both useful and usable. It is accessible to various stakeholders, provides interactive means to explore complex data, and is organised such that content can be absorbed at a glance (high-level overviews) or in depth (detailed drilldowns). Next, we will explore how the tool could be further enhanced with statistical analyses and visualisations, building on the current architecture and data to add even more value for users and evaluators.

7.1.7 Statistical Analyses and Visualizations

The statistics page presents a compact but meaningful set of metrics that dynamically adjust according to the filters applied by the user. At the top, the keyword frequency panel highlights the ten most recurring terms in programme descriptions, providing immediate insight into the thematic orientation of the available training. This is useful for both learners and policymakers: learners can quickly see whether a cluster of courses emphasizes "engineering," "students," or "risk management," while policymakers can detect patterns in how training providers frame their offerings and whether these align with strategic skills needs.

Figure 14. CYTIM Statistics view

The distribution by country chart visualizes how training opportunities are geographically spread, showing whether certain Member States are underrepresented. For a policymaker, this can highlight regional disparities and inform where new initiatives or funding should be directed, while for learners it indicates where training is available.

- The distribution by ECSF roles chart is particularly significant as it maps the courses against the European Cybersecurity Skills Framework, making it clear which professional roles (e.g., Incident Responder, Cybersecurity Architect, Legal/Policy Officer) are most supported. This allows jobseekers to assess whether training is available for their target career path and enables decision-makers to spot shortages in advanced or less common roles.
- The distribution by delivery mode chart illustrates how programmes are delivered, whether through in-person classes, hybrid models, or potentially online. This dimension is critical for accessibility: working professionals or learners in remote regions benefit most from hybrid or online options, while policymakers can track whether digital delivery channels are being adequately supported across Europe.
- The distribution by language chart reveals the linguistic accessibility of programmes, an important factor in widening participation and ensuring inclusivity across multilingual regions. Students can see whether programmes exist in their native or working language, and policymakers can detect where linguistic barriers might hinder uptake of training, supporting translation or localisation initiatives.

8 TRAINING REQUIREMENTS & CONCLUDING REMARKS

8.1 Training requirements

The CADMUS Project establishes a singular, evidence-based framework that each country chapter (Netherlands, Greece, Cyprus, Croatia) customises according to its labour market characteristics. The blueprint integrates quantitative skills-gap data with qualitative insights from CyberHubs, literature review, anticipatory trend analysis and focus groups, subsequently converting these inputs into modular, practice-oriented courses and trainings offered on a unified platform stack. All components are aligned with e-CF competences and responsibilities defined by ECSF cybersecurity profiles, to ensure European transferability and support for the Cyber Security Skills Academy.

Training priorities are established by combining:

- **GAP analyses** – cross-country tables that reveal the most significant competency shortages, with 'C.3. Education and Training Provision', 'D.9. Personnel Development', 'C.4. Problem Management' and 'D.1. Information Security Strategy Development' competences lacking the most.
- **CyberHubs** analysis shows that 'C.5. Systems Management', 'B.6. ICT Systems Engineering' and 'C.4. Problem Management' are demanded the most in Lithuania, Spain, Estonia, Slovenia, Greece, Hungary and Belgium.
- **Literature review** shows that ransomware, malware, social engineering and disinformation are trending cybersecurity threats across Europe, thereby highlighting the need for the improvement of employees' skills through training and education. Problem solving, system management and -testing, risk management and information security management are highly sought-after competences.
- **Trend analysis** reveals that EU-wide factors, including NIS2/DORA, accelerated cloud usage, and AI-driven threats which further underscore the need for enhanced compliance, vendor governance, and automation competences.
- **Focus group insights** reveal that employers and educators acknowledge existing shortages while also highlighting intricacies related to soft skills and AI threats, such as the need to "translate cloud risks for executives" and "collaborate across vendors."

The matrix below (Table AP) encapsulates the five beneficiary categories that the CADMUS curriculum is required to serve, correlating each with pertinent ECSF profile descriptions and the unique needs identified by GAP analyses, focus group insights, and trend analyses.

The people belonging to the target group 'under-represented groups' are not represented separately as a segment because they can belong to one or more of the above segments. Significantly, people in all segments need to recognise themselves in the wording of vacancies and educational offerings that appeal to them.

Segment	Typical role profiles	Key drivers
SMEs & start-ups	Cybersecurity Implementer, Risk Manager	Acute shortage of hands-on secure-by-design skills and post-incident recovery know-how.
Public authorities, services and institutions	Cybersecurity Architect, Auditor	NIS-2 compliance, critical-infrastructure resilience, and OT security.
Educators, trainers and capacity builders	Cybersecurity Educator	There is a need for an integrated approach that combines modern teaching strategies with targeted technical capability enhancement, particularly in the areas of cybersecurity training and outreach for women in cyber.
Students and early-career pursuers	Cyber Threat-Intelligence Specialist, Digital-Forensics Investigator	Career-entry pathways: Request for practice-rich delivery modes.
Career changers, reskilling candidates and lifelong learners (Upskilling professionals)	CISO, Cybersecurity Consultant	Bridging business-security alignment gaps and soft-skill deficits.

Table AP. Five beneficiary categories of learners that the CADMUS curriculum is required to serve

CADMUS employs a hybrid, challenge-oriented training and education approach as outlined in Work Package 3 of the proposal:

- Cyber Range Scenarios (Capture-the-Flag, Defence Exercises).
- Serious Games and Table-Top Exercises.
- Bootcamps and traineeships that integrate online theoretical instruction with in-person design sprints.
- Instructor-led or self-directed short courses or training on the learning platform.

WP4 delineates an interoperable stack:

- Learning Management System (LMS) for content management, assessment, and open-badge issuance.
- CADMUS Cyber Range for consistent, automated technical laboratories.
- Serious Games & Table-Top Exercises (SG&TTX) engine for governance and policy simulations.

The selection of Learning Outcome Sets (LOS) adheres to two principles:

- Address the most significant quantitative skills gaps first — for instance, prioritise modules in Education and Training Provision and Personnel Development.

- Incorporate essential skills early — AI-driven threat detection, supply chain risk management, and operational technology security are pertinent even when present demand is subdued.

In line with the CADMUS backward-design approach, foundational EQF 4–5 disciplines (Cyber Fundamentals, Basic Network Security) are intentionally positioned to support vertical progression toward advanced EQF 6–7 specialisations, such as Incident Response and Secure-by-Design.

The selected LOS address persistent deficiencies identified in the evidence and align with the backward-design methodology used for CADMUS training.

- The "Overall Country Analysis" table (see Table AG) evaluates each e-CF competence based on the extent of the discrepancy between educational offerings and employer requirements. The most significant positive discrepancies, specifically 23% for ‘D.3. Education and Training Provision’, 11% for ‘D.9. Personnel Development’, and 10% ‘C.4. Problem Management’, serve as the initial criterion.
- For each green-gap competency, we examined key findings from the gap analysis in combination with the country reports, trend analysis and focus group statements. These affirm that the same competences (e.g., articulating cloud risks for executives, collaborating throughout vendor ecosystems) will become increasingly vital in the next three to five years.
- The paradigm necessitates that, from the identified gaps, we develop modular LOS (parent nodes), which can subsequently be disaggregated into distinct learning outcomes and levels of complexity (EQF).
- Each LOS is articulated in terminology consistent with the ECSF role profiles and the e-CF, ensuring that credits, badges, and curricula are identifiable throughout the EU.

The subsequent table (Table AQ) serves as a roadmap: it outlines current deficiencies, forecasts impending legislative and technological challenges, and provides curriculum designers with a framework for tiered, interoperable training modules in later stages of the project.

	LOS Title	What learners will be able to do	Training type & platform bundle	EQF level	Evidence (why this LOS)	Primary role
1	**Incident Response & Business Continuity (Problem Management)**	Detect, contain, and recover from ransomware; maintain critical ops.	Cyber-Range blue-team lab + incident SG&TTX; optional 2-3 days boot-camp.	5-6	C.4. sees double-digit (33% for courses and 37% for trainings) future relevance despite current oversupply; focus groups stress the need for tested run-books.	Incident Responder, SOC Analyst
2	**Zero-Trust Systems Management & Cloud Identity**	Deploy conditional access, micro-segment workloads, and run continuous posture assessments.	Guided Azure/AWS labs + SG&TTX "compromised M365 tenant" scenario.	5	C.5. shows (28% and 34% for courses and trainings) shortage; focus/trend stress "securing cloud environments, managing identities, enforcing zero-trust architectures".	Security Administrator, Cybersecurity Architect
3	**Basic Network & Endpoint Security**	Harden Small Office/Home Office (SOHO) routers, configure patching & logging.	Hands-on lab images + video walkthroughs.	4–5	Same focus-group evidence as #24; provides prereq for DevSecOps & IR LOS, in line with C.5. Systems Management (28% in courses and 34% in training).	Security Administrator
4	**Cyber-Education & Training Toolkit**	Design learner-centred labs; run awareness campaigns.	Mentor-guided design studio (LMS) +	4-7	D.3. gap (29% for both courses and trainings); educators in focus groups request ready-made modules and pedagogy refresh.	Cybersecurity Educator
5	**Risk Management**	Identify, analyse, and treat risk; quantify risk; draft and present mitigation plans.	Blended micro-credential (LMS) + workshop on risk register & KRIs + board-level tabletop briefing.	6-7	E.3. Risk Management (courses: 27%; trainings: 28%)	Risk Manager, CISO
6	**Pen-Testing & Ethical Hacking**	Plan & execute IoT/OT pentests; report Common Vulnerability Scoring System (CVSS) findings.	2-3 days boot-camp + red-team CTF arena.	5	B.3. Testing shortfall (in courses 21% and training 26%) and explicit call for OT/IoT pentest skills.	Penetration Tester, Vulnerability Assessor
7	**Security Management**	Establish and maintain an Information Security Management System (ISMS), incl. policies,	Instructor-led workshops + assignments on LMS	6-7	E.8. Information Security Management (courses 19%; trainings 20%)	Legal/Policy & Compliance Officer, Auditor, CISO

	LOS Title	What learners will be able to do	Training type & platform bundle	EQF level	Evidence (why this LOS)	Primary role
		controls, metrics; prepare audit evidence.				
8	**Capability Building**	Design workforce-development programmes (competency matrix, mentoring, career paths) and measure learning outcomes.	Mentor-guided “design studio” + competency-matrix workshop	5-6	D.9. Personnel Development (courses: 19%; trainings: 17%)	Cybersecurity Educator/Trainer, Team Lead
9	**Compliance-Driven Quality Management (NIS2/DORA/CRA)**	Map controls to obligations; prepare audit evidence.	Instructor-led workshops + document-trail assignment on LMS.	6	E.6. Quality Management & Compliance flagged as future-critical with a gap of 15% in courses and 18% in trainings; trend scan stresses regulatory wave.	Legal/Policy & Compliance Officer, Auditor
10	**OT / ICS Security Engineering**	Harden PLCs, design network segmentation, and perform firmware analysis for Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA).	Weekend field-lab in an emulated plant + cyber-range Real-Time Operating System (RTOS) images.	5–6	B.6. gap (courses 17% and trainings 15%) plus focus on "expertise in securing embedded systems, firmware analysis, and network segmentation".	Cybersecurity Architect, Security Operations Engineer, Cybersecurity Consultant
11	**Digital Forensics & Evidence Handling**	Acquire, preserve, and analyse digital evidence; testify in mock court.	Forensics lab images + virtual courtroom role-play.	5	Focus group column cites "analysing what happened after an attack, collecting digital evidence" under D.7. Science & Analysis (shows a 10% course gap on level e2 and 12% training gap on level e2)	Digital Forensics Investigator
12	**Malware Analysis & Reverse Engineering**	Deconstruct malicious binaries, identify behaviour, extract IoCs and build detection signatures; write short technical advisories.	Advanced sandbox lab (Sisyfos) on Cyber Range + self-paced LMS theory + virtual "malware zoo" for practice.	6–7	D.7. Science & Analysis shows a 12% and 19% gap in courses and training in CY, NL, and CR; focus groups call for "deep technical forensics" skills, and trend analysis flags AI-crafted malware and APT tooling.	Digital Forensics Investigator, Cybersecurity Researcher · Threat-Intelligence Specialist

	LOS Title	What learners will be able to do	Training type & platform bundle	EQF level	Evidence (why this LOS)	Primary role
13	**Secure Architecture & Cloud Sovereignty**	Design zero-trust, multi-cloud landing zones; document data flows for NIS2.	Design-studio sprints (virtual) + IaC lab on Cyber-Range.	6	A.5. Architecture Design shows a 14% gap in courses and training; the trend paper links sovereignty & cloud risk.	Cybersecurity Architect
14	**Security Strategy & Business Alignment**	Align security with corporate KPIs, craft multi-year roadmaps, and brief boards.	Case-based masterclass + CISO war-game (SG&TTX).	6–7	Deficits: D.1. (12% in courses and 13% in trainings) and A.1. (5% in courses and 6% in trainings); focus groups call these "least-covered yet most requested" leadership skills.	Chief Information Security Officer, Cybersecurity Consultant, Security Governance Manager
15	**Secure Documentation & Technical Writing**	Produce SBOMs, IR reports, and user-centric SOPs compliant with NIS2.	Collaborative writing clinic with peer review, supported by LMS.	4–5	B.5. shows (11% in courses and 14% in trainings) shortage and is in the CY top-five vacancies; public-sector focus on "clear, compliant communication".	Cybersecurity Trainer / Educator, Legal, Policy & Compliance Officer
16	**Secure Coding & Design**	Apply secure design patterns; perform threat-modelling; write/review code with proper secrets handling.	Instructor-led workshops + assignments on LMS	5-6	B.1. Application/Product Development (courses 12%, trainings 11%).	Secure Software Developer
17	**Security Consulting & Risk Communication**	Articulate technical risks in business language; brief executives; draft risk-mitigation roadmaps.	Blended micro-credential on LMS (+ live virtual class) + board-level table-top in SG&TTX engine.	6-7	The gap (8% and 13%) for D.12. in courses and trainings; focus groups call for "explaining cloud risks to decision-makers," and trend scan predicts gap widening.	Cybersecurity Consultant, CISO
18	**Stakeholder Relationship Management**	Coordinate multi-party security work (vendors, CERTs, legal) and nurture cyber-culture.	micro-credential (LMS) + role-play scenarios in SG&TTX.	6	The gap on both courses and trainings is 9% for E.4.; "work across departmental & vendor boundaries" flagged by both evidence streams.	Risk Manager, Compliance Officer
19	**Technology-Foresight & Innovation Management**	Run horizon scans, quantify tech-risk curves, pitch R&D pilots to execs.	Innovation sprint (virtual) + foresight canvas on Sisyfos LMS.	6	A.7. gap (8% and 9% in courses and training) and ranked top competence in the CY labour market.	Research & Development Specialist, Cybersecurity Consultant, Chief

	LOS Title	What learners will be able to do	Training type & platform bundle	EQF level	Evidence (why this LOS)	Primary role
						Information Security Officer
20	**Business Change Management & Cyber-Resilience**	Orchestrate secure migrations, embed resilience KPIs in change projects.	Instructor-led workshop + SG&TTX "merger-day cut-over" scenario.	6	E.7. flagged in trends for "aligning resilience and business continuity" with a 6% and 7% gap in courses and training.	Legal, Policy & Compliance Officer, Chief Information Security Officer
21	**Secure Component Integration & SBOM Management**	Integrate third-party labs, generate/validate SBOMs, and remediate supply-chain CVEs.	CI/CD pipeline lab + dependency-track toolchain.	5	B.2. gap 6% in both courses and trainings; EU trend: "enhanced incident reporting, stricter supply-chain oversight incl. SBOM requirements".	Secure Software Developer, Security Operations Engineer
22	**DevSecOps & Secure Deployment**	Embed SAST/SCA, IaC scanning, and SBOM export in CI/CD.	Guided GitLab pipelines in Cyber-Range + self-paced LMS units.	5-6	B.4. Solution Deployment & App Dev deficits between 4% and 6% for courses and trainings in the countries; focus on secure-by-design mandates (CRA).	Secure Software Developer, Security Engineer
23 - Focus Group	**Cyber Fundamentals & Digital Hygiene**	Apply MFA, backups, phishing spotting, and escalate incidents.	Self-paced micro-course + gamified quiz engine.	4	Focus groups highlight a fundamental skills gap in SMEs/education.	*Cross-cutting entry skill*
24 - Trend	**Post-Quantum Cryptography & Crypto-Agility**	Assess cryptographic inventories, plan migration to PQC algorithms, and maintain crypto-agility playbooks.	Self-paced LMS + cloud HSM lab + table-top "crypto swap" drill.	6–7	Trend scan flags "growing awareness in preparing for post-quantum cryptography" and the need for agile key rotation.	Secure Software Developer · Research & Development Specialist

Table AQ. Roadmap for the development of modular Learning Objectives Sets (LOS) to bridge the cybersecurity skills gap in the EU.

To guarantee a logical transition from recognised skills deficiencies to tangible training implementation, each Learning Outcome Set (LOS) chosen within the CADMUS project must be converted into a systematic format that supports curriculum development, platform integration, and pilot assessment. The template presented in Table AR is an example of a standardised instrument for disaggregating each Learning Outcome Statement (LOS) into specific training requirements, related learning outcomes, and assessment methodologies. It can function as a conduit between the overarching LOS definitions and the tangible execution of modular, interoperable, and EQF-compliant courses.

<table>
<tr><td>Training title (From master LOS table):</td><td></td></tr>
<tr><td>Target EQF Level(s):</td><td>☐ EQF 4 ☐ EQF 5 ☐ EQF 6 ☐ EQF 7</td></tr>
<tr><td>ECSF Role(s):</td><td>☐ CISO ☐ CRM ☐ CAU ☐ CAN
☐ CAR ☐ CIR ☐ DFI ☐ PT
☐ SOC ☐ CLPCO ☐ CTE ☐ CR
☐ _____</td></tr>
<tr><td>Target Audience</td><td>☐ SMEs/startups personnel
☐ Civil and Public Sector personnel
☐ Educators/trainers
☐ Graduate students
☐ Upskilling professionals</td></tr>
<tr><td>Specific job profiles</td><td></td></tr>
<tr><td>Learning Outcomes</td><td>
<table>
<tr><th>#</th><th>Learning Outcome</th><th>EQF Level</th><th>Assessment Process</th></tr>
<tr><td>1</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Delivery Components</td><td>
<table>
<tr><th>Component</th><th>Description</th></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Training Content</td><td>
<table>
<tr><th>LO Ref.</th><th>Key Topics</th><th>Recommended Method(s)</th><th>Content Type</th></tr>
<tr><td>1</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Evaluation</td><td>☐ Rubric-based evaluation
☐ Peer-review participation
☐ Platform-based activity logs</td></tr>
<tr><td>Additional Notes</td><td>Specify prerequisites, platform dependencies, certification/badge criteria, or trainers' requirements.</td></tr>
</table>

Table AR. Template for Learning Outcome Statement (LOS) into specific training requirements, related learning outcomes, and assessment methodologies

The project funded under Grant Agreement No. 101190006 is supported by the European Health and Digital Executive Agency (HaDEA)

Co-funded by the European Union

8.2 Concluding remarks on requirements

The 24 Learning-Outcome Sets enumerated in 'Training requirements' constitute more than a mere inventory; they provide the logical framework that will govern each subsequent work package (WP) in CADMUS.

- **WP3**: Each Learning Outcome Statement (LOS) now functions as a "parent node" that WP3 will disaggregate into detailed learning outcomes, credit allocations, and syllabi. Since each LOS possesses an EQF entry level and an ECSF mapping, curriculum developers can synchronise national qualifications and job-role expectations without further translation efforts.
- **WP4**: The LOS list delineates the course backlog for the adaptation of the all-in-one learning platform, which includes the construction of Cyber-Range scenarios, the upgrade of the Sisyfos platform, and the development of Serious-Game/Table-Top exercises (SG&TTX) platform. The task descriptions for T4.2–T4.4 expressly cite these three delivery pillars and will derive their technical requirements, assessment artifacts, and laboratory blueprints directly from the LOS specifications.
- **WP5**: National pilots will select a customised subset of LOS (e.g., "Security Consulting" for the Netherlands, "Incident Response" for Cyprus) and conduct evaluations with SMEs, civil personnel, and graduate groups. The integrated EQF levels facilitate mixed-ability groups, whereas the platform bundle tags (LMS, Cyber Range, SG&TTX) enable pilots to combine synchronous, asynchronous, and practical formats.
- **WP6**: Each Learning Outcome Set (LOS) is linked to a specific evidence statement (gap percentage, focus-group quotation, or trend driver), allowing WP6 to monitor whether pilot learners effectively bridge the identified competence gap and generate the anticipated artefacts as outlined in the LOS descriptions. That completes the connection between preliminary analytics and effect assessment.

The LOS table serves as the agreement between evidence and execution: it instructs designers on construction, developers on delivery, pilots on testing locations, and evaluators on success criteria. By anchoring each Learning Outcome Set in validated deficiencies and European-standard taxonomies, CADMUS guarantees that upcoming courses will be both demand-oriented and compatible across the EU.

Co-funded by the European Union

ANNEXES

Annex 1 Methodological details

Labelling vacancies and educational offerings

A more detailed overview of the labelling process and how to avoid common pitfalls is described here.

When labelling the texts, one must not only describe the vacancy or educational offering in terms of the required skills, as used in for instance word counting methods such as NLP, but also connect parts of the text to specific competences. Therefore, it is important that the vacancy does not vaguely reference a competence but instead clearly reflects it. Labelling is carried out at sentence level, as individual words do not provide enough context to describe competences accurately, and paragraphs may include several competences without sufficient distinction. A single sentence may contain multiple competences or a competence at several levels. For vacancies, typically, only two to five competences are selected as the "main" competences. This limited number ensures the relevance of the competences to the specific vacancy. In cases where a database of vacancies is filtered by competence, only those with a high level of compatibility will be shown. However, for educational courses a higher number of competences is possible, especially for programmes that span years such as bachelor's or master's degree.

The key factors in labelling competences are similar for vacancies and educational offers. For both, the leading factor in deciding whether to label a competence or not is the text of the vacancy or description of the course itself. While the vacancy text should ideally clearly guide the selection of key competences, this is not always the case. This is the same for descriptions of training goals and course content. By strictly applying the competence model the inference of the person labelling is limited, interpretation or 'guessing' should be minimal.

It is important that the correct competence proficiency level (1 through 5) is attached to each identified competence from the vacancy or education text. The proficiency levels are defined as:

> **Proficiency level 1**. *Able to apply knowledge and skills to solve straight-forward problems; responsible for own actions; operating in a stable environment.*
>
> **Proficiency level 2**. *Operates with reasonable capability and independence in specified boundaries and may supervise others in this environment; conceptual and abstract model building using limited creative thinking; uses theoretical knowledge and practical skills to solve problems within a predictable and sometimes unpredictable context.*
>
> **Proficiency level 3**. *Respected for innovative methods and use of initiative in specific technical or business areas; providing leadership and taking responsibility for team performances and development in unpredictable environments.*

Co-funded by the European Union

Proficiency level 4. *Extensive scope of responsibilities deploying specialised integration capability in complex environments; full responsibility for strategic development of staff working in unfamiliar and unpredictable situations.*

Proficiency level 5. *Overall accountability and responsibility; recognised inside and outside the organisation for innovative solutions and for shaping the future using outstanding leading edge thinking and knowledge.*

ECSF Role Analysis

The first analytical approach focuses on improving the precision of vacancy-to-ECSF role matching for the twelve existing ECSF roles. This is achieved by evaluating how closely the for the analysis utilised vacancies match each ECSF role based on their designated competences and their associated competency levels. A match rate is calculated for each vacancy by comparing its listed competences and their levels with those defined in each ECSF role. The more closely they align, the higher the match rate. This analysis allows the classification of vacancies into three categories:

1. Identical or high-matching: Vacancies that fully align (75%-100% match) with an ECSF role, meaning they have a close to identical competency range and identical task ranges, which are determined by comparing the vacancy description and the ECSF role's task definition. These suggest the current role definition is appropriate and does not require modification within the context of the used database.
2. Closely aligned: Vacancies that show a match (50%-75%), indicating minor gaps. This suggests the addition or removal of specific competences or adjustment of their levels to improve alignment, provided the vacancy is matching the ECSF role's definition.
3. Significantly divergent: High-matching vacancies that share few or no core similarities with the existing ECSF role beyond the core competences and their levels. This signals a need for more substantial restructuring of the role definition, potentially involving a re-evaluation of several competences.

To identify patterns in vacancy-to-ECSF role alignment, this report analyses a minimum of five top-matching vacancies per ECSF role. Among these, at least two vacancies must clearly correspond with the role's conceptual definition, not just in terms of competency overlap, but also in terms of task and role function. Each vacancy is therefore reviewed individually to determine whether the match is truly representative of the ECSF role, or whether it results merely from overlapping competences without a functional match. If multiple high-matching vacancies genuinely align with the ECSF role in terms of both competences and functional scope, adjustments will be considered to increase overall match rating with fitting vacancies. Conversely, if high-matching vacancies consistently deviate from the ECSF role's intended definition, this signals a need to revise the role's assigned competences. Such revisions aim to improve alignment with the relevant vacancies found in the database that clearly match the role's conceptual intent but currently fall outside the top matching rate. This analysis ensures that the current ECSF roles reflect identified job requirements with higher accuracy and relevance.

The second approach aims to identify specific representative shortcomings of the current ECSF roles, meaning to identify and adjust the ECSF roles' definitional competences or their

Co-funded by the European Union

competence levels adapting them to their labour market demands. Additionally, this approach aims to develop potential new ECSF roles which address identified existing or developing gaps in labour market coverage. By contrasting labour market competence demand with ECSF competences, gaps of competency coverage can be identified. Competences that are frequently in demand but not currently covered by existing ECSF roles are traced back to the relevant vacancies. These vacancies are then analysed for recurring patterns in competency demand, competence levels, and task descriptions.
If consistent commonalities emerge across the analysed vacancies, and an overarching role can be defined that encompasses them, a recommendation is made to develop a new ECSF role based on these findings. This process ensures that the ECSF remains responsive to evolving labour market demands.

Co-funded by
the European Union

Annex 2 Example vacancy labelling based on e-CF

As the Information Security Officer, you will serve as the point of contact for information security matters across the company. You will be responsible for maintaining and continuously improving the company's Information Security Management System (ISMS), ensuring compliance with relevant standards and regulations. In this role, you will lead risk assessments, coordinate internal and external audits, manage security policies and procedures, and oversee awareness training programs. You will also drive cross-functional improvement initiatives and provide expert guidance to departments, helping to strengthen the company's overall security posture. This role reports to the Head of Information Security. Introduction / context

E9, level 4

E3, level 4
E6, level 4
E8, level 4
D3, level 3
D12, level 4

- Develop, maintain, and document information security policies and procedures, ensuring they remain up to date, compliant with regulations, and easily accessible to all employees.
- Communicate policy updates and procedural changes across the organization to ensure alignment and awareness.
- Support the execution of the information security strategy, including the coordination and facilitation of internal and external audits.
- Conduct regular risk assessments to identify vulnerabilities and areas for improvement and take proactive steps to mitigate identified risks.
- Organize and lead periodic awareness training programs to educate employees on security protocols, compliance requirements, and threat prevention strategies.
- Act as a central point of contact for all information security-related matters, providing guidance and support to various departments.
- Lead and oversee security improvement initiatives and projects across the organization to strengthen overall information security posture.
- Investigate information security incidents, perform root cause analyses, and coordinate the implementation of corrective and preventive actions. Responsibilities

E8, level 4

E8, level 4
E6, level 4

E3, level 4

D3, level 3

D12, level 4

E8, level 4

E9, level 4

- A Bachelor's, Master's, or HBO degree in Computer Science, Engineering, or a related field.
- A minimum of 3 years of experience in Information Security, Risk Management, and Compliance.
- Solid knowledge of security frameworks, IT management practices, and GDPR requirements.
- Hands-on experience with security audits and assessments, particularly in relation to ISO 27001.
- Familiarity with industry standards and regulations such as ISO 27001, GDPR, and NIS2, as well as information security management systems.
- Working knowledge of common security tools and technologies, including firewalls, IDS, antivirus, and others, is considered a strong plus.
- Fluency in English, both written and spoken.
- Agile, proactive, and analytical mindset, with strong problem-solving capabilities.
- A curious and innovative approach to tackling challenges with practical and creative solutions.
- Excellent communication and collaboration skills, with the ability to work effectively across different cultures and backgrounds. Job requirements

E6, level 4

E6, level 4
E9, level 4

What's in for you

- Working for a Great Place to Work® certified company;
- Opportunities to develop your skills even further through training and certifications;
- High quality laptop/desktop, monitor, work phone, noise cancelling headphones, and any other equipment necessary for your role;
- An international team of 30+ nationalities, full of high-performance colleagues you can exchange experiences with and learn from. Details company workplace

Co-funded by the European Union

Annex 3 Step-by-step guide for labelling vacancies with competences

1. Carefully read the entire job listing or educational offering. For vacancies, consider who the employer is, their overall goals, and how this position contributes to those objectives. For educational offerings, consider the proposed learning outcomes and in which context the knowledge and skills are supposed to be applied.
2. Highlight or copy the sentences that describe key tasks/learning outcomes.
3. Focus on the verbs used in the job listing or programme description. It is important to distinguish between verbs such as plan, build, run, enable, and manage, as each signals different expectations. Based on this, competences can be identified within one of the five categories outlined in the e-Competence Framework.
4. Identify the primary categories (plan, build, run, enable, manage) of the job listing or educational programme.
5. Select preferably four to six competences that best reflect the demands of the role or programme and apply these to the highlighted sentences. Keep in mind that important competences may fall outside the primary categories, so consider these as well. Be as specific as possible when assigning competences.
6. Determine the appropriate proficiency level for each competence by considering the explanation provided, the job requirements/educational level, the years/level of experience required, and the nature of the role/educational offering. The level is based on both complexity and the degree of ingenuity expected.

Co-funded by
the European Union

Annex 4 Manual vacancies Excel sheet format

The purpose of the Excel Sheet Format Vacancies is to provide a systematic way to label and score (cybersecurity) vacancies according to the e-CF. The Excel Sheet works as follows. First, each vacancy is to be inserted into the Excel Sheet according to their description data, such as 'vacancy title', 'vacancy description' and 'organisation'. Consequently, each vacancy is to be scored according to the e-CF competence framework. After each vacancy's competence is identified, labelled and scored, the Excel Sheet automatically scores the competences according to twelve ECSF profiles. The percentages indicate to what extent the vacancy's competences match the competences of the ECSF roles. For example, if a vacancy has a 40% match with the ECSF role Chief Information Security Officer, this means that 40% of the competences of the vacancy are proficient enough for the role of Chief Information Security Officer.
To provide guidance and overview, each column from the Excel Sheet Format Vacancies is highlighted and an explanation is given what data needs to be inserted:

Column Name	Column Explanation	Column Example
Vacancy Title	Input the full title of the vacancy	Manager Incident Response
Vacancy Description	Input the first two sentences of the vacancy description. The rest of the vacancy description must be stored in a separate file (word, pdf, etc.) with a matching Identification Number.	No example provided
Identification Number	The identification number is a unique code that contains both the identification of the vacancy and coupled documents. This allows for the storing of vacancy descriptions and related documents in a database. **Format**: VNL00000000000001_20250307_1 **Differentiation between vacancies and education**: V for vacancies, E for education (see format Excel Sheet Education) **Unique land code**: e.g. NL, CY, GR, HR **Vacancy identification (14 numbers)**: e.g. 00000000000001 **Underscore**: _ **Date**: Closing date of vacancy. E.g. 7 March 2025 translates to 20250307 **Underscore**: _ **Attached documents**: e.g. one attached document translates to 1	VNL00000000000001_20250307_1
Organisation(s)	Input the organisation(s) that has/have posted the vacancy.	Ministry of Foreign Affairs

Co-funded by the European Union

Speaking Language	Input the required speaking language(s) of the vacancy. If multiple languages are required use a '/' between the languages. E.g. Dutch/English.	English Dutch/English Dutch/English/German
Location (country, city)	Input the country and city where the vacancy is situated. Use a ',' between country and city. E.g. Netherlands, Amsterdam.	Netherlands, Amsterdam England, London
Part time / full time / hours	Input whether the vacancy is either part time or full time. Additionally provide the number of working hours per week. Use '()' for the number of hours. E.g. Full time (40 hours). If it is not clear whether the vacancy is part time or full time, for example when an estimation of hours is mentioned, first use 'or' between part time and full time and a '-' between the number of hours. E.g. Part time or full time (32-40 hours).	Full time (40 hours) Part time (32 hours) Part time or full time (32-40 hours)
Level	Input the experience level (Junior, Medior, Senior) of the vacancy: Junior (0-3 years experience) Medior (3-5 years experience) Senior (5+ years experience)	Junior Medior Senior
URL	Input the URL of the vacancy.	No example provided
e-Competence Framework	Input the e-CF competences which are deduced from the vacancy. Utilise the competence manual for guidance. Each e-CF competence and related proficiency level has its own separate column. E.g. 'A.1. Information Systems and Business Strategy Alignment' Proficiency level 4. For each deduced e-CF competence input the correct proficiency level.	1 2 3 4 5
ECSF Role	There are twelve ECSF roles, e.g. Chief Information Security Officer. Once e-CF competences of a vacancy are imported into the document, the competences are automatically scored against the ECSF roles. These columns **do not** have to be filled in manually.	Different percentages

Co-funded by the European Union

Annex 5 Manual education initiatives Excel sheet format

The Excel Sheet Format Education Initiatives functions the same way as the Excel Sheet Format Vacancies. The differences between both documents are the data input and the descriptive columns.

Column Name	Column Explanation	Column Example
Education Title	Input the full title of the education initiative	Software Developer
Education Description	Input the first two sentences of the education description. The rest of the education description must be stored in a separate file (word, pdf, etc.) with a matching Identification Number.	No example provided
Identification Number	The identification number is a unique code that contains both the identification of the education initiative and coupled documents. This allows for the storing of education initiative descriptions and related documents in a database. **Format**: ENL00000000000001_20250307_1 **Differentiation between vacancies and education**: E for education, V for vacancies, (see format Excel Sheet Vacancies) **Unique land code**: e.g. NL, CY, GR, HR **Education identification (14 numbers)**: e.g. 00000000000001 **Underscore**: _ **Date**: Closing date of education initiative. E.g. 7 March 2025 translates to 20250307 **Underscore**: _ **Attached documents**: e.g. one attached document translates to 1	ENL00000000000001_20250307_1
Education, Course Training (ECT)	Input whether the education initiative can be classified as 'education', 'course' or 'training' **Education** Duration: minimum of one year Receive: formal degree **Course** Duration: minimum five hours Receive: certificate	Education Course Training

Co-funded by the European Union

	Training Duration: one to five hours Receive: participatory certificate	
ECT Form	Input the ECT form 'class', 'online' or 'hybrid	Class Online Hybrid
ECT Provider	Input the ECT provider	MBO Utrecht
Education Load (hours)	Input the education load in terms of hours	40 hours
Education Duration	Input the education duration in terms of 'hours', 'days' or 'years'	1 Hour 2 Days 3 Years
Speaking Language	Input the required speaking language of the education initiative	Dutch English
Location (country, city)	Input the country and city where the education initiative is situated. Use a ',' between country and city. E.g. Netherlands, Amsterdam.	Netherlands, Amsterdam England, London
URL	Input the URL of the education initiative	No example provided
e-CF Competence Framework	Input the e-CF competences which are deduced from the education initiative. Utilise the competence manual for guidance. Each e-CF competence and related proficiency level has its own separate column. E.g. 'A.1. Information Systems and Business Strategy Alignment' Proficiency level 4. For each deduced e-CF competence input the correct proficiency level.	1 2 3 4 5
ECSF Role	There are twelve ECSF roles, e.g. Chief Information Security Officer. Once e-CF competences of an education initiative are imported into the document, the competences are automatically scored against the ECSF roles. These columns **do not** have to be filled in manually.	Different percentages

Co-funded by the European Union

Annex 6 Tables, figures & data

Vacancy Tables – The Netherlands

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				21	8
A.2. Service Level Management			3	5	
A.3. Business Plan Development			4	11	3
A.4. Product / Service Planning		1	4	5	
A.5. Architecture Design			27	7	7
A.6. Application / Product Design	1	3	21		
A.7. Technology Trend Monitoring			23	27	4
A.8. Sustainability Management			0	0	
A.9.Innovating				14	2
A.10. User Experience		1	6	6	
B.1. Application / Product Development	4	19	47		
B.2. Component Integration		4	6	3	
B.3. Testing	0	9	24	0	
B.4. Solution Deployment	0	7	10		
B.5. Documentation Production	0	11	23		
B.6. ICT Systems Engineering			27	10	
C.1. User Support	1	19	4		
C.2. Change Support		4	7		
C.3. Service Delivery	1	11	13		
C.4. Problem Management		10	44	13	
C.5. Systems Management	0	14	45		
D.1. Information Security Strategy Development				28	10
D.2. Quality Strategy Development				13	1
D.3. Education and Training Provision		5	32		
D.4. Purchasing		0	1	3	
D.5. Sales Development		0	12	4	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		10	44	37	4
D.8. Contract Management		0	2	3	
D.9. Personnel Development		3	21	9	
D.10. Information and Knowledge Management			10	14	5
D.11. Needs Identification			17	25	3
D.12. Security Consulting			61	83	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		3	9	19	5
E.3. Risk Management		4	11	13	
E.4. Relationship Management			57	54	

Co-funded by the European Union

E.5. Process Improvement			8	3	
E.6. Quality Management and Compliance		0	26	20	
E.7. Business Change Management			4	13	2
E.8. Information Security Management		1	23	31	
E.9. Information Systems Governance				13	0

Table 1. The Netherlands - Labour market needs according to competence and proficiency level

Competence / Proficiency level		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	D.12. Security Consulting	10,43%	29,81%
2	E.4. Relationship Management	8,04%	22,98%
3	D.7. Science and Analysis	6,88%	19,67%
4	B.1. Application / Product Development	5,07%	14,49%
5	C.4. Problem Management	4,86%	13,87%
6	C.5. Systems Management	4,28%	12,22%
7	E.8. Information Security Management	3,99%	11,39%
8	A.7. Technology Trend Monitoring	3,91%	11,18%
9	E.6. Quality Management and Compliance	3,33%	9,52%
10	D.11. Needs Identification	3,26%	9,32%
11	A.5. Architecture Design	2,97%	8,49%
12	D.1. Information Security Strategy Development	2,75%	7,87%
13	B.6. ICT Systems Engineering	2,68%	7,66%
14	D.3. Education and Training Provision	2,68%	7,66%
15	E.2. Project and Portfolio Management	2,61%	7,45%
16	B.5. Documentation Production	2,46%	7,04%
17	B.3. Testing	2,39%	6,83%
18	D.9. Personnel Development	2,39%	6,83%
19	A.1. IS and Business Strategy Alignment	2,10%	6,00%
20	D.10. Information and Knowledge Management	2,10%	6,00%
21	E.3. Risk Management	2,03%	5,80%
22	A.6. Application / Product Design	1,81%	5,18%
23	C.3. Service Delivery	1,81%	5,18%
24	C.1. User Support	1,74%	4,97%
25	E.7. Business Change Management	1,38%	3,93%
26	A.3. Business Plan Development	1,30%	3,73%
27	B.4. Solution Deployment	1,23%	3,52%
28	A.9. Innovating	1,16%	3,31%
29	D.5. Sales Development	1,16%	3,31%
30	D.2. Quality Strategy Development	1,01%	2,90%

Co-funded by the European Union

31	A.10. User Experience	0,94%	2,69%
32	B.2. Component Integration	0,94%	2,69%
33	E.9. Information Systems Governance	0,94%	2,69%
34	E.5. Process Improvement	0,80%	2,28%
35	A.4. Product / Service Planning	0,72%	2,07%
36	A.2. Service Level Management	0,58%	1,66%
37	C.2. Change Support	0,58%	1,66%
38	D.8. Contract Management	0,36%	1,04%
39	D.4. Purchasing	0,29%	0,83%
40	A.8. Sustainability Management	0,00%	0,00%
41	D.6. Digital Marketing	0,00%	0,00%
42	E.1. Forecast Development	0,00%	0,00%

Table 2. The Netherlands - Competences from vacancy descriptions according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				5	1
A.2. Service Level Management			3	0	
A.3. Business Plan Development			0	3	2
A.4. Product/Service Planning		0	1	2	
A.5. Architecture Design			10	0	1
A.6. Application/Product Design	0	2	4		
A.7. Technology Trend Monitoring			3	5	0
A.8. Sustainability Management			0	0	
A.9. Innovating				3	0
A.10. User Experience		0	1	4	
B.1. Application/Product Development	2	8	13		
B.2. Component Integration		2	2	0	
B.3. Testing	0	3	3	0	
B.4. Solution Deployment	0	1	2		
B.5. Documentation Production	0	4	6		
B.6. ICT Systems Engineering			9	3	
C.1. User Support	1	4	1		
C.2. Change Support		0	0		
C.3. Service Delivery	0	2	3		
C.4. Problem Management		5	10	3	
C.5. Systems Management	0	7	12		
D.1. Information Security Strategy Development				9	2
D.2. Quality Strategy Development				1	1
D.3. Education and Training Provision		1	5		
D.4. Purchasing		0	0	1	

Co-funded by the European Union

D.5. Sales Development		0	4	1	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		1	10	6	1
D.8. Contract Management		0	1	0	
D.9. Personnel Development		0	4	4	
D.10. Information and Knowledge Management			2	1	2
D.11. Needs Identification			6	6	1
D.12. Security Consulting			15	30	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		1	1	2	1
E.3. Risk Management		0	3	1	
E.4. Relationship Management			8	15	
E.5. Process Improvement			3	0	
E.6. Quality Management and Compliance		0	4	6	
E.7. Business Change Management			1	2	0
E.8. Information Security Management		0	7	6	
E.9. Information Systems Governance				2	0

Table 3. The Netherlands - SME labour market needs according to competence and level

Competence / Proficiency level		Percentage of frequency within total number of SME competences	Percentage of frequency within SME vacancies
1	D.12. Security Consulting	13,47%	38,79%
2	B.1. Application/Product Development	6,89%	19,38%
3	E.4. Relationship Management	6,89%	19,38%
4	C.5. Systems Management	5,69%	16,38%
5	C.4. Problem Management	5,39%	15,52%
6	D.7. Science and Analysis	3,89%	15,52%
7	D.11. Needs Identification	3,89%	11,21%
8	E.8. Information Security Management	3,89%	11,21%
9	B.6. ICT Systems Engineering	3,89%	10,34%
10	A.5. Architecture Design	3,59%	9,48%
11	D.1. Information Security Strategy Development	3,29%	9,48%
12	B.5. Documentation Production	2,99%	8,62%
13	E.6. Quality Management and Compliance	2,99%	8,62%
14	A.7. Technology Trend Monitoring	2,40%	6,90%
15	D.9. Personnel Development	2,40%	6,90%
16	A.1. IS and Business Strategy Alignment	1,80%	5,17%
17	A.6. Application/Product Design	1,80%	5,17%
18	B.3. Testing	1,80%	5,17%
19	C.1. User Support	1,80%	5,17%

Co-funded by the European Union

20	D.3. Education and Training Provision	1,80%	5,17%
21	A.3. Business Plan Development	1,50%	4,31%
22	A.10. User Experience	1,50%	4,31%
23	C.3. Service Delivery	1,50%	4,31%
24	D.5. Sales Development	1,50%	4,31%
25	D.10. Information and Knowledge Management	1,50%	4,31%
26	E.2. Project and Portfolio Management	1,50%	4,31%
27	B.2. Component Integration	1,20%	3,45%
28	E.3. Risk Management	1,20%	3,45%
29	A.2. Service Level Management	0,90%	2,59%
30	A.4. Product/Service Planning	0,90%	2,59%
31	A.9. Innovating	0,90%	2,59%
32	B.4. Solution Deployment	0,90%	2,59%
33	E.5. Process Improvement	0,90%	2,59%
34	E.7. Business Change Management	0,90%	2,59%
35	D.2. Quality Strategy Development	0,60%	1,72%
36	E.9. Information Systems Governance	0,60%	1,72%
37	D.4. Purchasing	0,30%	0,86%
38	D.8. Contract Management	0,30%	0,86%
39	A.8. Sustainability Management	0,00%	0,00%
40	C.2. Change Support	0,00%	0,00%
41	D.6. Digital Marketing	0,00%	0,00%
42	E.1. Forecast Development	0,00%	0,00%

Table 4. The Netherlands - Competences within SME vacancies according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				8	5
A.2. Service Level Management			0	0	
A.3. Business Plan Development			1	3	0
A.4. Product/Service Planning		1	2	2	
A.5. Architecture Design			5	4	3
A.6. Application/Product Design	0	1	7		
A.7. Technology Trend Monitoring			7	15	3
A.8. Sustainability Management			0	0	
A.9. Innovating				4	0
A.10. User Experience		0	1	1	
B.1. Application/Product Development	2	3	12		
B.2. Component Integration		0	0	2	
B.3. Testing	0	3	6	0	

Co-funded by the European Union

B.4. Solution Deployment	0	4	1		
B.5. Documentation Production	0	1	7		
B.6. ICT Systems Engineering			5	2	
C.1. User Support	0	7	0		
C.2. Change Support		0	0		
C.3. Service Delivery	0	7	1		
C.4. Problem Management		3	9	5	
C.5. Systems Management	0	1	14		
D.1. Information Security Strategy Development				8	3
D.2. Quality Strategy Development				2	0
D.3. Education and Training Provision		0	9		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	4	2	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		2	15	14	1
D.8. Contract Management		0	0	3	
D.9. Personnel Development		2	9	3	
D.10. Information and Knowledge Management			5	4	2
D.11. Needs Identification			6	5	1
D.12. Security Consulting			20	24	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	4	9	2
E.3. Risk Management		0	1	1	
E.4. Relationship Management			22	16	
E.5. Process Improvement			3	1	
E.6. Quality Management and Compliance		0	9	5	
E.7. Business Change Management			0	3	0
E.8. Information Security Management		1	4	8	
E.9. Information Systems Governance				7	0

Table 5. The Netherlands - Public Professional labour market needs according to competence and level

Competence / Proficiency level		Percentage of frequency within total number of public professional competences	Percentage of frequency within public professional vacancies
1	D.12. Security Consulting	10,81%	29,73%
2	E.4. Relationship Management	9,34%	25,68%
3	D.7. Science and Analysis	7,86%	21,62%
4	A.7. Technology Trend Monitoring	6,14%	16,89%
5	B.1. Application/Product Development	4,18%	11,49%
6	C.4. Problem Management	4,18%	11,49%
7	C.5. Systems Management	3,69%	10,14%

Co-funded by the European Union

8	E.2. Project and Portfolio Management	3,69%	10,14%
9	D.9. Personnel Development	3,44%	9,46%
10	E.6. Quality Management and Compliance	3,44%	9,46%
11	A.1. IS and Business Strategy Alignment	3,19%	8,78%
12	E.8. Information Security Management	2,19%	8,78%
13	A.5. Architecture Design	2,95%	8,11%
14	D.11. Needs Identification	2,95%	8,11%
15	D.1. Information Security Strategy Development	2,70%	7,43%
16	D.10. Information and Knowledge Management	2,70%	7,43%
17	B.3. Testing	2,21%	6,08%
18	D.3. Education and Training Provision	2,21%	6,08%
19	A.6. Application/Product Design	1,97%	5,41%
20	B.5. Documentation Production	1,97%	5,41%
21	C.3. Service Delivery	1,97%	5,41%
22	B.6. ICT Systems Engineering	1,72%	4,73%
23	C.1. User Support	1,72%	4,73%
24	E.9. Information Systems Governance	1,72%	4,73%
25	D.5. Sales Development	1,47%	4,05%
26	A.4. Product/Service Planning	1,23%	3,38%
27	B.4. Solution Deployment	1,23%	3,38%
28	A.3. Business Plan Development	0,98%	2,70%
29	A.9. Innovating	0,98%	2,70%
30	D.8. Contract Management	0,74%	2,03%
31	E.5. Process Improvement	0,74%	2,03%
32	E.7. Business Change Management	0,74%	2,03%
33	A.10. User Experience	0,49%	1,35%
34	B.2. Component Integration	0,49%	1,35%
35	D.2. Quality Strategy Development	0,49%	1,35%
36	E.3. Risk Management	0,49%	1,35%
37	A.2. Service Level Management	0,00%	0,00%
38	A.8. Sustainability Management	0,00%	0,00%
39	C.2. Change Support	0,00%	0,00%
40	D.4. Purchasing	0,00%	0,00%
41	D.6. Digital Marketing	0,00%	0,00%
42	E.1. Forecast Development	0,00%	0,00%

Table 6. The Netherlands - Competences within Public Professionals vacancies according to percentual frequency

Co-funded by the European Union

ECSF Role		%match	St. Dev.	#No1	#No 2	#No3
1	Cyber Threat Intelligence Specialist	6,46%	10,36%	84	44	12
2	Cybersecurity Implementer	4,97%	10,76%	69	20	9
3	Cybersecurity Educator	4,76%	13,15%	53	7	1
4	Cybersecurity Architect	4,31%	9,70%	55	26	7
5	Cyber, Legal, Policy & Compliance Officer	4,14%	9,84%	50	25	1
6	Cybersecurity Researcher	3,93%	8,46%	59	24	7
7	Cyber Incident Responder	3,39%	7,83%	23	42	12
8	Cybersecurity Auditor	3,39%	8,54%	27	36	8
9	Chief Information Security Officer (CISO)	3,39%	8,44%	42	26	5
10	Digital Forensics Investigator	2,69%	7,91%	38	11	2
11	Cybersecurity Risk Manager	2,43%	7,75%	32	9	3
12	Penetration Tester	1,78%	5,69%	8	20	9

Table 7. The Netherlands - ECSF Roles, average, standard deviation and top 3 within vacancies

Co-funded by the European Union

Vacancy Tables – Greece

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment			0	18	
A.2. Service Level Management					
A.3. Business Plan Development					
A.4. Product/ Service Planning					
A.5. Architecture Design			97	0	27
A.6. Application/ Product Design			124		
A.7. Technology Trend Monitoring			29	15	4
A.8. Sustainability Management					
A.9. Innovating					4
A.10. User Experience					
B.1. Application/ Product Development			124	0	
B.2. Component Integration		28	0	18	
B.3. Testing			152	32	
B.4. Solution Deployment		18	0	0	
B.5. Documentation Production			61	0	
B.6. ICT Systems Engineering		0	0	124	
C.1. User Support					
C.2. Change Support					
C.3. Service Delivery					
C.4. Problem Management		0	4	28	
C.5. Systems Management					
D.1. Information Security Strategy Development			0	18	15
D.2. Quality Strategy Development					
D.3. Education and Training Provision			3		
D.4. Purchasing					
D.5. Sales Development					
D.6. Digital Marketing					
D.7. Science and Analysis			0	8	
D.8. Contract Management					
D.9. Personnel Development			3		
D.10. Information and Knowledge Management			4	3	
D.11. Needs Identification					
D.12. Security Consulting			248	65	
E.1. Forecast Development					
E.2. Project and Portfolio Management					
E.3. Risk Management		0	2	52	
E.4. Relationship Management		0	3		
E.5. Process Improvement		0	8		
E.6. Quality Management and Compliance		0	5	9	

Co-funded by the European Union

E.7. Business Change Management				4	
E.8. Information Security Management			20	30	
E.9. Information Systems Governance				24	15

Table 8. Greece - Labour market needs according to competence and proficiency level

	ECSF Role	%match	St.Dev.	#No1	#No2	#No3
1	Cybersecurity Implementer	48,71%	46,71%	99	20	29
2	Cybersecurity Architect	42,18%	40,04%	19	99	30
3	Cyber Incident Responder	24,27%	29,34%	29	2	118
4	Cybersecurity Auditor	15,32%	26,53%	12	33	41
5	Penetration Tester	14,84%	27,93%	18	12	39
6	Digital Forensics Investigator	12,90%	22,67%	2	29	29
7	Chief Information Security Officer (CISO)	10,32%	25,01%	15	0	8
8	Cybersecurity Risk Manager	9,78%	20,15%	8	1	32
9	Cyber Legal, Policy & Compliance Officer	8,97%	27,36%	20	9	0
10	Cyber Threat Intelligence Specialist	8,55%	15,28%	3	4	30
11	Cybersecurity Educator	3,90%	13,98%	3	20	0
12	Cybersecurity Researcher	1,86%	12,76%	4	0	0

Table 9. Greece - ECSF Roles, average, standard deviation and top 3 within vacancies

Co-funded by the European Union

Vacancy Tables – Cyprus

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				0	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			1	0	0
A.4. Product/ Service Planning		0	0	0	
A.5. Architecture Design			6	5	0
A.6. Application/ Product Design	0	2	0		
A.7. Technology Trend Monitoring			6	17	0
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		0	0	0	
B.1. Application/ Product Development	0	1	0		
B.2. Component Integration		0	0	0	
B.3. Testing	4	8	2	0	
B.4. Solution Deployment	1	13	0		
B.5. Documentation Production	4	14	0		
B.6. ICT Systems Engineering			4	1	
C.1. User Support	3	2	0		
C.2. Change Support		0	0		
C.3. Service Delivery	1	0	0		
C.4. Problem Management		6	16	0	
C.5. Systems Management	0	4	0		
D.1. Information Security Strategy Development				13	0
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		13	1		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		14	1	0	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	0	
D.10. Information and Knowledge Management			0	1	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			15	0	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	0	0	0
E.3. Risk Management		6	4	0	
E.4. Relationship Management			2	0	
E.5. Process Improvement			0	1	
E.6. Quality Management and Compliance		3	5	0	

Co-funded by the European Union

E.7. Business Change Management			0	0	0
E.8. Information Security Management		1	4	0	
E.9. Information Systems Governance				2	1

Table 10. Cyprus - Labour market needs according to competence and proficiency level

Competence / proficiency level		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	A.7. Technology Trend Monitoring	11,11%	56,1%
2	C.4. Problem Management	10,14%	51,22%
3	B.5. Documentation Production	8,70%	43,90%
4	D.7. Science and Analysis	7,25%	36,59%
5	D.12. Security Consulting	7,25%	36,59%
6	B.3. Testing	6,76%	34,15%
7	B.4. Solution Deployment	6,76%	34,15%
8	D.3. Education and Training Provision	6,76%	34,15%
9	D.1. Information Security Strategy Development	6,28%	31,71%
10	A.5. Architecture Design	5,31%	26.83%
11	E.3. Risk Management	4,83%	24,39%
12	E.6. Quality Management and Compliance	3,86%	19,51%
13	B.6. ICT Systems Engineering	2,42%	12,20%
14	C.1. User Support	2,42%	12,20%
15	E.8. Information Security Management	2,42%	12,20%
16	C.5. Systems Management	1,93%	9,76%
17	E.9. Information Systems Governance	1,45%	7,32%
18	A.6. Application/ Product Design	0,97%	4,88%
19	E.4. Relationship Management	0,97%	4,88%
20	A.3. Business Plan Development	0,48%	2,44%
21	B.1. Application/ Product Development	0,48%	2,44%
22	C.3. Service Delivery	0,48%	2,44%
23	D.10. Information and Knowledge Management	0,48%	2,44%
24	E.5. Process Improvement	0,48%	2,44%
25	A.1. IS and Business Strategy Alignment	0,0%	0.0%
26	A.2. Service Level Management	0,0%	0.0%
27	A.4. Product/ Service Planning	0,0%	0.0%
28	A.8. Sustainability Management	0,0%	0.0%
29	A.9. Innovating	0,0%	0.0%
30	A.10. User Experience	0,0%	0.0%
31	B.2. Component Integration	0,0%	0.0%
32	C.2. Change Support	0,0%	0.0%
33	D.2. Quality Strategy Development	0,0%	0.0%
34	D.4. Purchasing	0,0%	0.0%

Co-funded by the European Union

35	D.5. Sales Development	0,0%	0.0%
36	D.6. Digital Marketing	0,0%	0.0%
37	D.8. Contract Management	0,0%	0.0%
38	D.9. Personnel Development	0,0%	0.0%
39	D.11. Needs Identification	0,0%	0.0%
40	E.1. Forecast Development	0,0%	0.0%
41	E.2. Project and Portfolio Management	0,0%	0.0%
42	E.7. Business Change Management	0,0%	0.0%

Table 11. Cyprus - Competences from vacancy descriptions according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				0	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			1	0	0
A.4. Product/Service Planning		0	0	0	
A.5. Architecture Design			6	5	0
A.6. Application/Product Design	0	2	0		
A.7. Technology Trend Monitoring			6	4	0
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		0	0	0	
B.1. Application/Product Development	0	1	0		
B.2. Component Integration		0	0	0	
B.3. Testing	4	8	2	0	
B.4. Solution Deployment	1	1	0		
B.5. Documentation Production	4	2	0		
B.6. ICT Systems Engineering			4	1	
C.1. User Support	3	2	0		
C.2. Change Support		0	0		
C.3. Service Delivery	1	0	0		
C.4. Problem Management		5	4	0	
C.5. Systems Management	0	4	0		
D.1. Information Security Strategy Development				1	0
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		1	1		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		2	1	0	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	0	

Co-funded by the European Union

D.10. Information and Knowledge Management			0	1	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			3	0	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	0	0	0
E.3. Risk Management		6	3	0	
E.4. Relationship Management			2	0	
E.5. Process Improvement			0	1	
E.6. Quality Management and Compliance		3	5	0	
E.7. Business Change Management			0	0	0
E.8. Information Security Management		1	4	0	
E.9. Information Systems Governance				1	1

Table 12. Cyprus - SME labour market needs according to competence and level

Competence / Proficiency level		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	B.3. Testing	12,96%	48,28%
2	A.5. Architecture Design	10,19%	37,93%
3	A.7. Technology Trend Monitoring	9,26%	34,48%
4	C.4. Problem Management	8,33%	31,03%
5	E.3. Risk Management	8,33%	31,03%
6	E.6. Quality Management and Compliance	7,41%	27,59%
7	B.5. Documentation Production	5,56%	20,69%
8	B.6. ICT Systems Engineering	4,63%	17,24%
9	C.1. User Support	4,63%	17,24%
10	E.8. Information Security Management	4,63%	17,24%
11	C.5. Systems Management	3,70%	13,79%
12	D.7. Science and Analysis	2,78%	10,34%
13	D.12. Security Consulting	2,78%	10,34%
14	A.6. Application/ Product Design	1,85%	6,90%
15	B.4. Solution Deployment	1,85%	6,90%
16	D.3. Education and Training Provision	1,85%	6,90%
17	E.4. Relationship Management	1,85%	6,90%
18	E.9. Information Systems Governance	1,85%	6,90%
19	A.3. Business Plan Development	0,93%	3,45%
20	B.1. Application/ Product Development	0,93%	3,45%
21	C.3. Service Delivery	0,93%	3,45%
22	D.1. Information Security Strategy Development	0,93%	3,45%
23	D.10. Information and Knowledge Management	0,93%	3,45%

Co-funded by the European Union

24	E.5. Process Improvement	0,93%	3,45%
25	A.1. IS and Business Strategy Alignment	0,0%	0,0%
26	A.2. Service Level Management	0,0%	0,0%
27	A.4. Product/ Service Planning	0,0%	0,0%
28	A.8. Sustainability Management	0,0%	0,0%
29	A.9. Innovating	0,0%	0,0%
30	A.10. User Experience	0,0%	0,0%
31	B.2. Component Integration	0,0%	0,0%
32	C.2. Change Support	0,0%	0,0%
33	D.2. Quality Strategy Development	0,0%	0,0%
34	D.4. Purchasing	0,0%	0,0%
35	D.5. Sales Development	0,0%	0,0%
36	D.6. Digital Marketing	0,0%	0,0%
37	D.8. Contract Management	0,0%	0,0%
38	D.9. Personnel Development	0,0%	0,0%
39	D.11. Needs Identification	0,0%	0,0%
40	E.1. Forecast Development	0,0%	0,0%
41	E.2. Project and Portfolio Management	0,0%	0,0%
42	E.7. Business Change Management	0,0%	0,0%

Table 13. Cyprus - Competences within SME vacancies according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				0	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/Service Planning		0	0	0	
A.5. Architecture Design			0	0	0
A.6. Application/Product Design	0	0	0		
A.7. Technology Trend Monitoring			0	12	0
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		0	0	0	
B.1. Application/Product Development	0	0	0		
B.2. Component Integration		0	0	0	
B.3. Testing	0	0	0	0	
B.4. Solution Deployment	0	12	0		
B.5. Documentation Production	0	12	0		
B.6. ICT Systems Engineering			0	0	
C.1. User Support	0	0	0		
C.2. Change Support		0	0		

Co-funded by the European Union

C.3. Service Delivery	0	0	0		
C.4. Problem Management		0	12	0	
C.5. Systems Management	0	0	0		
D.1. Information Security Strategy Development				12	0
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		12	0		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		12	0	0	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	0	
D.10. Information and Knowledge Management			0	0	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			12	0	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	0	0	0
E.3. Risk Management		0	0	0	
E.4. Relationship Management			0	0	
E.5. Process Improvement			0	0	
E.6. Quality Management and Compliance		0	0	0	
E.7. Business Change Management			0	0	0
E.8. Information Security Management		0	0	0	
E.9. Information Systems Governance				0	0

Table 14. Cyprus - Public Professional labour market needs according to competence and level

Competence / proficiency level		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	A.7. Technology Trend Monitoring	12.5%	100.0%
2	B.4. Solution Deployment	12.5%	100.0%
3	B.5. Documentation Production	12.5%	100.0%
4	C.4. Problem Management	12.5%	100.0%
5	D.1. Information Security Strategy Development	12.5%	100.0%
6	D.3. Education and Training Provision	12.5%	100.0%
7	D.7. Science and Analysis	12.5%	100.0%
8	D.12. Security Consulting	12.5%	100.0%
9	A.1. IS and Business Strategy Alignment	0.0%	0.0%
10	A.2. Service Level Management	0.0%	0.0%
11	A.3. Business Plan Development	0.0%	0.0%
12	A.4. Product/Service Planning	0.0%	0.0%
13	A.5. Architecture Design	0.0%	0.0%

Co-funded by the European Union

14	A.6. Application/Product Design	0.0%	0.0%
15	A.8. Sustainability Management	0.0%	0.0%
16	A.9. Innovating	0.0%	0.0%
17	A.10. User Experience	0.0%	0.0%
18	B.1. Application/Product Development	0.0%	0.0%
19	B.2. Component Integration	0.0%	0.0%
20	B.3. Testing	0.0%	0.0%
21	B.6. ICT Systems Engineering	0.0%	0.0%
22	C.1. User Support	0.0%	0.0%
23	C.2. Change Support	0.0%	0.0%
24	C.3. Service Delivery	0.0%	0.0%
25	C.5. Systems Management	0.0%	0.0%
26	D.2. Quality Strategy Development	0.0%	0.0%
27	D.4. Purchasing	0.0%	0.0%
28	D.5. Sales Development	0.0%	0.0%
29	D.6. Digital Marketing	0.0%	0.0%
30	D.8. Contract Management	0.0%	0.0%
31	D.9. Personnel Development	0.0%	0.0%
32	D.10. Information and Knowledge Management	0.0%	0.0%
33	D.11. Needs Identification	0.0%	0.0%
34	E.1. Forecast Development	0.0%	0.0%
35	E.2. Project and Portfolio Management	0.0%	0.0%
36	E.3. Risk Management	0.0%	0.0%
37	E.4. Relationship Management	0.0%	0.0%
38	E.5. Process Improvement	0.0%	0.0%
39	E.6. Quality Management and Compliance	0.0%	0.0%
40	E.7. Business Change Management	0.0%	0.0%
41	E.8. Information Security Management	0.0%	0.0%
42	E.9. Information Systems Governance	0.0%	0.0%

Table 15. Cyprus - Competences within Public Professionals vacancies according to percentual frequency

	ECSF Role	%match	St.Dev.	#No1	#No2	#No3
1	Digital Forensics Investigator	13.41%	12.47%	22	0	0
2	Cyber Incident Responder	9.76%	10.0%	0	19	1
3	Cybersecurity Implementer	4.39%	9.38%	4	3	1
4	Cyber, Legal, Policy & Compliance Officer	4.27%	9.41%	3	4	0
5	Cybersecurity Educator	3.25%	9.89%	4	0	0
6	Chief Information Security Officer (CISO)	2.93%	7.07%	2	3	1
7	Cybersecurity Researcher	1.95%	5.93%	2	1	1
8	Cybersecurity Risk Manager	1.83%	6.51%	2	1	0
9	Cybersecurity Architect	1.46%	6.83%	1	0	1

Co-funded by the European Union

10	Cyber Threat Intelligence Specialist	0.98%	4.31%	0	2	0
11	Penetration Tester	0.49%	3.09%	0	1	0
12	Cybersecurity Auditor	0.00%	0.00%	0	0	0

Table 16. Cyprus - ECSF Roles, average, standard deviation and top 3 within vacancies

Co-funded by the European Union

Vacancy Tables – Croatia

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				13	1
A.2. Service Level Management			1	2	
A.3. Business Plan Development			1	1	1
A.4. Product/ Service Planning		1	2	0	
A.5. Architecture Design			10	6	3
A.6. Application/ Product Design	0	1	2		
A.7. Technology Trend Monitoring			8	1	1
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		1	0	0	
B.1. Application/ Product Development	4	4	3		
B.2. Component Integration		6	6	8	
B.3. Testing	0	12	4	0	
B.4. Solution Deployment	0	5	8		
B.5. Documentation Production	15	28	7		
B.6. ICT Systems Engineering			6	9	
C.1. User Support	3	18	4		
C.2. Change Support		12	7		
C.3. Service Delivery	0	4	4		
C.4. Problem Management		9	27	1	
C.5. Systems Management	2	12	10		
D.1. Information Security Strategy Development				28	5
D.2. Quality Strategy Development				5	2
D.3. Education and Training Provision		15	13		
D.4. Purchasing		6	2	0	
D.5. Sales Development		2	3	0	
D.6. Digital Marketing		0	0	1	
D.7. Science and Analysis		6	1	1	0
D.8. Contract Management		4	2	0	
D.9. Personnel Development		1	3	1	
D.10. Information and Knowledge Management			13	2	0
D.11. Needs Identification			8	4	0
D.12. Security Consulting			16	14	
E.1. Forecast Development			2	0	
E.2. Project and Portfolio Management		3	10	2	1
E.3. Risk Management		6	20	8	
E.4. Relationship Management			4	1	
E.5. Process Improvement			8	0	
E.6. Quality Management and Compliance		0	2	2	

Co-funded by the European Union

E.7. Business Change Management			0	1	1
E.8. Information Security Management		3	19	10	
E.9. Information Systems Governance				4	3

Table 17. Croatia - Labour market needs according to competence and proficiency level

Competence / Proficiency level		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	B.5. Documentation Production	8,90%	60,98%
2	C.4. Problem Management	6,58%	45,12%
3	E.3. Risk Management	6,05%	41,46%
4	D.1. Information Security Strategy Development	5,87%	40,24%
5	E.8. Information Security Management	5,69%	39,02%
6	D.12. Security Consulting	5,34%	36,59%
7	D.3. Education and Training Provision	4,98%	34,15%
8	C.1. User Support	4,45%	30,49%
9	C.5. Systems Management	4,27%	29,27%
10	B.2. Component Integration	3,56%	24,39%
11	A.5. Architecture Design	3,38%	23,17%
12	C.2. Change Support	3,38%	23,17%
13	B.3. Testing	2,85%	19,51%
14	E.2. Project and Portfolio Management	2,85%	19,51%
15	B.6. ICT Systems Engineering	2,67%	18,29%
16	D.10. Information and Knowledge Management	2,67%	18,29%
17	A.1. IS and Business Strategy Alignment	2,49%	17,07%
18	B.4. Solution Deployment	2,31%	15,85%
19	D.11. Needs Identification	2,14%	14,63%
20	B.1. Application/ Product Development	1,96%	13,41%
21	A.7. Technology Trend Monitoring	1,78%	12,20%
22	C.3. Service Delivery	1,42%	9,76%
23	D.4. Purchasing	1,42%	9,76%
24	D.7. Science and Analysis	1,42%	9,76%
25	E.5. Process Improvement	1,42%	9,76%
26	D.2. Quality Strategy Development	1,25%	8,54%
27	E.9. Information Systems Governance	1,25%	8,54%
28	D.8. Contract Management	1,07%	7,32%
29	D.5. Sales Development	0,89%	6,10%
30	D.9. Personnel Development	0,89%	6,10%
31	E.4. Relationship Management	0,89%	6,10%
32	E.6. Quality Management and Compliance	0,71%	4,88%
33	A.2. Service Level Management	0,53%	3,66%
34	A.3. Business Plan Development	0,53%	3,66%

Co-funded by the European Union

35	A.4. Product/ Service Planning	0,53%	3,66%
36	A.6. Application/ Product Design	0,53%	3,66%
37	E.1. Forecast Development	0,36%	2,44%
38	E.7. Business Change Management	0,36%	2,44%
39	A.10. User Experience	0,18%	1,22%
40	D.6. Digital Marketing	0,18%	1,22%
41	A.8. Sustainability Management	0,00%	0,00%
42	A.9. Innovating	0,00%	0,00%

Table 18. Croatia - Competences from vacancy descriptions according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				3	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/ Service Planning		0	0	0	
A.5. Architecture Design			3	1	2
A.6. Application/ Product Design	0	0	1		
A.7. Technology Trend Monitoring			0	0	0
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		1	0	0	
B.1. Application/ Product Development	2	0	2		
B.2. Component Integration		2	3	4	
B.3. Testing	0	2	3	0	
B.4. Solution Deployment	0	1	3		
B.5. Documentation Production	8	7	2		
B.6. ICT Systems Engineering			2	6	
C.1. User Support	2	6	2		
C.2. Change Support		5	3		
C.3. Service Delivery	0	2	1		
C.4. Problem Management		3	10	1	
C.5. Systems Management	1	4	7		
D.1. Information Security Strategy Development				9	3
D.2. Quality Strategy Development				0	1
D.3. Education and Training Provision		7	1		
D.4. Purchasing		1	2	0	
D.5. Sales Development		1	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		2	1	1	0
D.8. Contract Management		1	1	0	

Co-funded by the European Union

D.9. Personnel Development		0	1	0	
D.10. Information and Knowledge Management			6	0	0
D.11. Needs Identification			3	1	0
D.12. Security Consulting			6	5	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		2	0	1	1
E.3. Risk Management		2	5	1	
E.4. Relationship Management			0	1	
E.5. Process Improvement			3	0	
E.6. Quality Management and Compliance		0	0	0	
E.7. Business Change Management			0	0	1
E.8. Information Security Management		0	3	2	
E.9. Information Systems Governance				1	0

Table 19. Croatia - SME labour market needs according to competence and level

Competence / Proficiency level		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	B.5. Documentation Production	9,39%	58,62%
2	C.4. Problem Management	7,73%	48,28%
3	C.5. Systems Management	6,63%	41,38%
4	D.1. Information Security Strategy Development	6,63%	41,38%
5	D.12. Security Consulting	6,08%	37,93%
6	C.1. User Support	5,52%	34,48%
7	B.2. Component Integration	4,97%	31,03%
8	B.6. ICT Systems Engineering	4,42%	27,59%
9	C.2. Change Support	4,42%	27,59%
10	D.3. Education and Training Provision	4,42%	27,59%
11	E.3. Risk Management	4,42%	27,59%
12	A.5. Architecture Design	3,31%	20,69%
13	D.10. Information and Knowledge Management	3,31%	20,69%
14	B.3. Testing	2,76%	17,24%
15	E.8. Information Security Management	2,76%	17,24%
16	B.1. Application/ Product Development	2,21%	13,79%
17	B.4. Solution Deployment	2,21%	13,79%
18	D.7. Science and Analysis	2,21%	13,79%
19	D.11. Needs Identification	2,21%	13,79%
20	E.2. Project and Portfolio Management	2,21%	13,79%
21	A.1. IS and Business Strategy Alignment	1,66%	10,34%
22	C.3. Service Delivery	1,66%	10,34%
23	D.4. Purchasing	1,66%	10,34%
24	E.5. Process Improvement	1,66%	10,34%

Co-funded by the European Union

25	D.8. Contract Management	1,10%	6,90%
26	A.6. Application/ Product Design	0,55%	3,45%
27	A.10. User Experience	0,55%	3,45%
28	D.2. Quality Strategy Development	0,55%	3,45%
29	D.5. Sales Development	0,55%	3,45%
30	D.9. Personnel Development	0,55%	3,45%
31	E.4. Relationship Management	0,55%	3,45%
32	E.7. Business Change Management	0,55%	3,45%
33	E.9. Information Systems Governance	0,55%	3,45%
34	A.2. Service Level Management	0,00%	0,00%
35	A.7. Technology Trend Monitoring	0,00%	0,00%
36	A.3. Business Plan Development	0,00%	0,00%
37	A.4. Product/ Service Planning	0,00%	0,00%
38	A.8. Sustainability Management	0,00%	0,00%
39	A.9. Innovating	0,00%	0,00%
40	D.6. Digital Marketing	0,00%	0,00%
41	E.1. Forecast Development	0,00%	0,00%
42	E.6. Quality Management and Compliance	0,00%	0,00%

Table 20. Croatia - Competences within SME vacancies according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				3	0
A.2. Service Level Management			1	0	
A.3. Business Plan Development			0	0	0
A.4. Product/ Service Planning		1	0	0	
A.5. Architecture Design			2	0	0
A.6. Application/ Product Design	0	1	1		
A.7. Technology Trend Monitoring			1	0	0
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		0	0	0	
B.1. Application/ Product Development	0	2	1		
B.2. Component Integration		0	2	0	
B.3. Testing	0	3	0	0	
B.4. Solution Deployment	0	0	0		
B.5. Documentation Production	0	6	1		
B.6. ICT Systems Engineering			0	0	
C.1. User Support	0	0	2		
C.2. Change Support		2	1		
C.3. Service Delivery	0	0	2		
C.4. Problem Management		0	1	0	

Co-funded by the European Union

C.5. Systems Management	0	0	1		
D.1. Information Security Strategy Development				5	0
D.2. Quality Strategy Development				2	0
D.3. Education and Training Provision		1	3		
D.4. Purchasing		4	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		0	0	0	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	0	
D.10. Information and Knowledge Management			3	0	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			2	1	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		1	5	0	0
E.3. Risk Management		2	1	5	
E.4. Relationship Management			1	0	
E.5. Process Improvement			3	0	
E.6. Quality Management and Compliance		0	1	0	
E.7. Business Change Management			0	0	0
E.8. Information Security Management		1	3	2	
E.9. Information Systems Governance				0	1

Table 21. Croatia - Public Professional labour market needs according to competence and level

Competence / Proficiency level		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	E.3. Risk Management	9,88%	88,89%
2	B.5. Documentation Production	8,64%	77,78%
3	E.2. Project and Portfolio Management	7,41%	66,67%
4	E.8. Information Security Management	7,41%	66,67%
5	D.1. Information Security Strategy Development	6,17%	55,55%
6	D.3. Education and Training Provision	4,94%	44,44%
7	D.4. Purchasing	4,94%	44,44%
8	A.1. IS and Business Strategy Alignment	3,70%	33,33%
9	B.1. Application/ Product Development	3,70%	33,33%
10	B.3. Testing	3,70%	33,33%
11	C.2. Change Support	3,70%	33,33%
12	D.10. Information and Knowledge Management	3,70%	33,33%
13	D.12. Security Consulting	3,70%	33,33%
14	E.5. Process Improvement	3,70%	33,33%

Co-funded by the European Union

15	A.5. Architecture Design	2,47%	22,22%
16	A.6. Application/ Product Design	2,47%	22,22%
17	B.2. Component Integration	2,47%	22,22%
18	C.1. User Support	2,47%	22,22%
19	C.3. Service Delivery	2,47%	22,22%
20	D.2. Quality Strategy Development	2,47%	22,22%
21	A.2. Service Level Management	1,23%	11,11%
22	A.4. Product/ Service Planning	1,23%	11,11%
23	A.7. Technology Trend Monitoring	1,23%	11,11%
24	C.4. Problem Management	1,23%	11,11%
25	C.5. Systems Management	1,23%	11,11%
26	E.4. Relationship Management	1,23%	11,11%
27	E.6. Quality Management and Compliance	1,23%	11,11%
28	E.9. Information Systems Governance	1,23%	11,11%
29	A.8. Sustainability Management	0,00%	0,00%
30	A.9. Innovating	0,00%	0,00%
31	A.10. User Experience	0,00%	0,00%
32	B.4. Solution Deployment	0,00%	0,00%
33	B.6. ICT Systems Engineering	0,00%	0,00%
34	D.5. Sales Development	0,00%	0,00%
35	D.6. Digital Marketing	0,00%	0,00%
36	D.7. Science and Analysis	0,00%	0,00%
37	D.8. Contract Management	0,00%	0,00%
38	D.9. Personnel Development	0,00%	0,00%
39	D.11. Needs Identification	0,00%	0,00%
40	E.1. Forecast Development	0,00%	0,00%
41	A.3. Business Plan Development	0,00%	0,00%
42	E.7. Business Change Management	0,00%	0,00%

Table 22. Croatia - Competences within Public Professionals vacancies according to percentual frequency

	ECSF Role	%match	St.Dev.	#No1	#No2	#No3
1	Cyber, Legal, Policy & Compliance Officer	19,27%	20,40%	21	19	5
2	Cybersecurity Educator	14,23%	20,84%	18	8	4
3	Digital Forensics Investigator	10,67%	13,54%	12	13	4
4	Cybersecurity Researcher	10,24%	11,79%	11	14	9
5	Cybersecurity Implementer	6,83%	14,39%	9	3	5
6	Chief Information Security Officer (CISO)	6,59%	12,90%	4	7	7
7	Penetration Tester	6,59%	12,52%	5	6	4
8	Cybersecurity Auditor	6,59%	12,90%	4	6	6
9	Cyber Incident Responder	6,34%	11,21%	3	12	5
10	Cybersecurity Risk Manager	6,10%	11,42%	4	6	8

Co-funded by the European Union

11	Cyber Threat Intelligence Specialist	6,10%	10,21%	0	9	10
12	Cybersecurity Architect	5,12%	12,81%	5	3	4

Table 23. Croatia - ECSF Roles, average, standard deviation and top 3 within vacancies

Co-funded by the European Union

Tables – CyberHubs

Country / Skills	Lithuania	Spain	Estonia	Slovenia	Greece	Hungary	Belgium	e-CF
Data Privacy	X	X	X		X	X		E.6.
Access Control / Identity Management	X		X				X	C.5., E.9.
Network Security / Cyber Resilience	X	X		X	X			B.6., C.4., C.5.
Soft Skills		X		X	X	X	X	X
Hard Skills		X						X
Incident Management		X	X		X			C.4., E.3.
Cloud security		X	X		X	X	X	B.6., C.5., E.8.
Threat analysis			X					C.4., D.7., E.3.,
Network and System administration and integration		X	X					B.2., B.5., B.6.
Supply Chain Security		X						C.4., E.3.

Table 24. (Cyber)security skills (demand by cybersecurity labour market)

Country / Cybersecurity & ECSF roles	Lithuania	Spain	Estonia	Slovenia	Greece	Hungary	Belgium
Cybersecurity Auditor	X		X		X		
Cybersecurity Educator	X						
Cyber Incident Responder	X	X	X	X	X	X	X
CISO			X	X	X	X	X
Cybersecurity Architect		X	X		X	X	X
Cybersecurity Implementer	X	X	X	X	X	X	X
Cyber Legal Policy and Compliance Officers		X	X				X
Cybersecurity Risk Manager		X				X	
Cyber Threat Intelligence Officers			X				
Cybersecurity Researchers			X		X		
Ethical hacker/penetration tester					X		

Table 25. ECSF & Cybersecurity roles (demand by cybersecurity labour market)

Co-funded by the European Union

Tables – Literature review EU projects

Key issues affecting cybersecurity education	Coupled e-CF competences	Explanation
Poor interaction and lack of cooperation with industry	E.4. Relationship Management	Increase cooperation amongst industry organisations.
Lack of cybersecurity educators and training resources	D.3. Education and Training Provision	Educating (new) cybersecurity professionals.
The set of skills for cybersecurity professionals is changing due to altering cyberattacks	D.9. Personnel Development	Increasing focus on soft skills for cybersecurity professionals, such as Relationship Management, Project and Portfolio Management, Needs Identification
Lack of awareness of cybersecurity risks	D.3. Education and Training Provision D.9. Personnel Development	Enhance cybersecurity awareness. Enhance cybersecurity awareness.
Poor understanding of the labour market	A.4. Product/Service Planning A.7. Technology Trend Monitoring D.9. Personnel Development	Increase awareness of existing cybersecurity products and services. Increase understanding of existing cybersecurity technologies. Train personnel to understand the cybersecurity labour market.

Table 26. Identified key issues affecting cybersecurity education coupled to e-CF competences

Country / Trends	Lithuania	Spain	Estonia	Slovenia	Greece	Hungary	Belgium
Cybersecurity professionals require a mix of hard / soft skills	X		X	X	X	X	X
Cybersecurity skills gap between curricula of educational institutions and market demand	X			X	X	X	
Prioritisation of practical experience over degrees			X				
Prioritisation of cybersecurity certificates over traditional university degrees	X						
Lack of cybersecurity professionals		X		X		X	X
Increasingly sophisticated cyber threats due to geopolitical tensions	X	X	X	X			
Cyber-security experts 'export' to other countries		X					
Cyber-security experts 'import' from other countries			X				
Higher demand for cybersecurity specialist because of new (international) cs guidelines (e.g. NIS2)	X		X	X		X	X
Higher demand for cybersecurity specialist because of the growing adoption of technologies, such as cloud technologies, artificial	X	X					X

Co-funded by the European Union

intelligence, machine learning and blockchain technologies							
More attention for ethical behaviour in cyber & AI			X				

Table 27. CyberHubs: Identified trends

Cybersecurity threat	Coupled e-CF competences	Competence explanation
Ransomware	B.3. Testing C.4. Problem Management C.5. System Management E.3. Risk Management E.8. Information Security Management	Malware attack simulations (red teaming). Find a solution for the ransomware attack. Decide which solutions are important to implement. Manage/mitigate the ransomware attack. Manage information systems to prevent ransomware attack.
Malware	B.1. Application Development B.3. Testing C.4. Problem Management C.5. System Management E.3. Risk Management E.8. Information Security Management	Software-based design (source-code, scripts, firewalls). Malware attack simulations. Find a solution for the malware attack. Decide which solutions are important to implement. Manage/mitigate the malware attack. Manage information systems to prevent malware attack.
Social engineering	D.1. Information Security Strategy Development D.3. Education and Training Provision D.9. Personnel Development E.3. Risk Management	Development of a strategy to prevent social engineering from affecting the organisation. Enhance cybersecurity awareness. Enhance cybersecurity awareness. Enhance physical security awareness.
Threats against data	B.3. Testing C.4. Problem Management C.5. System Management E.3. Risk Management E.8. Information Security Management	Test the data environment. Find a solution for data breaches / data leaks. Decide which solutions are important to implement. Manage/mitigate data breaches / data leaks. Manage information systems to prevent data breaches / data leaks.
Threats against availability and integrity of data	B.3. Testing B.6. ICT Systems Engineering C.4. Problem Management C.5. Systems Management D.10. Information and Knowledge Management E.8. Information Security Management	DDoS attack simulations. Secure coupling of systems and data streams. Find a solution for the DDoS attack. Decide which solutions are important to implement in case of a DDoS attack. Create infrastructure for the organisation of data to minimise the influence of DDoS attacks. Manage information systems to prevent affecting the availability and integrity of data.
Disinformation and misinformation	D.1. Information Security Strategy Development D.3. Education and Training Provision D.9. Personnel Development	Development of a strategy to prevent disinformation and misinformation from affecting the organisation. Enhance cybersecurity awareness. Enhance cybersecurity awareness.
Supply chain attacks	A.5. Architecture Design C.4. Change Support E.3. Risk Management E.7. Business Change Management	Design the supply chain architecture. Support with operational problems within changing supply chain environments. Manage supply chain data streams and related risks. Manage a change in supply chain architecture.

Table 28. Identified cybersecurity threats coupled to e-CF competences

Co-funded by the European Union

Education Tables – The Netherlands

Competence / Proficiency level	e1	e2	e3	e4	e5
A.1. IS and Business Strategy Alignment				16	4
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	2
A.4. Product/ Service Planning		1	0	0	
A.5. Architecture Design			15	9	7
A.6. Application/ Product Design	0	1	13		
A.7. Technology Trend Monitoring			18	6	7
A.8. Sustainability Management			5	0	
A.9. Innovating				1	2
A.10. User Experience		0	9	0	
B.1. Application/ Product Development	1	6	16		
B.2. Component Integration		6	8	4	
B.3. Testing	2	10	24	8	
B.4. Solution Deployment	1	7	18		
B.5. Documentation Production	1	3	17		
B.6. ICT Systems Engineering			15	13	
C.1. User Support	1	3	0		
C.2. Change Support		4	4		
C.3. Service Delivery	0	5	6		
C.4. Problem Management		5	22	12	
C.5. Systems Management	3	5	34		
D.1. Information Security Strategy Development				20	6
D.2. Quality Strategy Development				6	0
D.3. Education and Training Provision		0	6		
D.4. Purchasing		0	1	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		2	19	13	0
D.8. Contract Management		0	0	1	
D.9. Personnel Development		3	2	2	
D.10. Information and Knowledge Management			1	4	0
D.11. Needs Identification			10	2	1
D.12. Security Consulting			18	4	
E.1. Forecast Development			5	0	
E.2. Project and Portfolio Management		1	1	1	3
E.3. Risk Management		7	34	23	
E.4. Relationship Management			11	6	
E.5. Process Improvement			8	4	
E.6. Quality Management and Compliance		5	27	11	

Co-funded by the European Union

E.7. Business Change Management			8	3	2
E.8. Information Security Management		21	35	37	
E.9. Information Systems Governance				21	9

Table 29. The Netherlands – Total training, course and education market supply according to competence and proficiency level

Trainings, Courses, Education		Percentage of frequency within total number of competences	Within education offerings
1	E.8. Information Security Management	11,86%	63,27%
2	E.3. Risk Management	8,16%	43,54%
3	B.3. Testing	5,61%	29,93%
4	E.6. Quality Management and Compliance	5,48%	29,25%
5	C.5. Systems Management	5,36%	28,57%
6	C.4. Problem Management	4,97%	26,53%
7	D.7. Science and Analysis	4,34%	23,13%
8	A.5. Architecture Design	3,95%	21,09%
9	A.7. Technology Trend Monitoring	3,95%	21,09%
10	E.9. Information Systems Governance	3,83%	20,41%
11	B.6. ICT Systems Engineering	3,57%	19,05%
12	B.4. Solution Deployment	3,32%	17,69%
13	D.1. Information Security Strategy Development	3,32%	17,69%
14	B.1. Application/ Product Development	2,93%	15,65%
15	D.12. Security Consulting	2,81%	14,97%
16	B.5. Documentation Production	2,68%	14,29%
17	A.1. IS and Business Strategy Alignment	2,55%	13,61%
18	B.2. Component Integration	2,30%	12,24%
19	E.4. Relationship Management	2,17%	11,56%
20	A.6. Application/ Product Design	1,79%	9,52%
21	D.11. Needs Identification	1,66%	8,84%
22	E.7. Business Change Management	1,66%	8,84%
23	E.5. Process Improvement	1,53%	8,16%
24	C.3. Service Delivery	1,40%	7,48%
25	A.10. User Experience	1,15%	6,12%
26	C.2. Change Support	1,02%	5,44%
27	D.9. Personnel Development	0,89%	4,76%
28	D.2. Quality Strategy Development	0,77%	4,08%
29	D.3. Education and Training Provision	0,77%	4,08%
30	E.2. Project and Portfolio Management	0,77%	4,08%
31	A.8. Sustainability Management	0,64%	3,40%
32	D.10. Information and Knowledge Management	0,64%	3,40%
33	E.1. Forecast Development	0,64%	3,40%
34	C.1. User Support	0,51%	2,72%

Co-funded by the European Union

35	A.9. Innovating	0,38%	2,04%
36	A.3. Business Plan Development	0,26%	1,36%
37	A.4. Product/ Service Planning	0,13%	0,68%
38	D.4. Purchasing	0,13%	0,68%
39	D.8. Contract Management	0,13%	0,68%
40	A.2. Service Level Management	0,0%	0,0%
41	D.5. Sales Development	0,0%	0,0%
42	D.6. Digital Marketing	0,0%	0,0%

Table 30. The Netherlands - Competences from education, training and course descriptions according to percentual frequency

Class/online/hybrid	Class	Class %	Online	Online %	Hybrid	Hybrid %
A.1. IS and Business Strategy Alignment	14	2,90%	7	2,59%	3	2,05%
A.2. Service Level Management	0	0,0%	0	0,0%	0	0,0%
A.3. Business Plan Development	0	0,0%	2	0,74%	0	0,0%
A.4. Product/ Service Planning	1	0,21%	1	0,37%	0	0,0%
A.5. Architecture Design	16	3,32%	10	3,70%	9	6,16%
A.6. Application/ Product Design	11	2,28%	2	0,74%	1	0,68%
A.7. Technology Trend Monitoring	22	4,56%	6	2,22%	4	2,74%
A.8. Sustainability Management	5	1,04%	0	0,0%	0	0,0%
A.9. Innovating	1	0,21%	2	0,74%	0	0,0%
A.10. User Experience	9	1,87%	0	0,0%	0	0,0%
B.1. Application/ Product Development	20	4,15%	4	1,48%	1	0,68%
B.2. Component Integration	10	2,07%	4	1,48%	4	2,74%
B.3. Testing	24	4,98%	20	7,41%	9	6,16%
B.4. Solution Deployment	20	4,15%	8	2,96%	2	1,37%
B.5. Documentation Production	11	2,28%	7	2,22%	3	2,05%
B.6. ICT Systems Engineering	17	3,53%	10	3,70%	7	4,79%
C.1. User Support	4	0,83%	0	0,0%	0	0,0%
C.2. Change Support	3	0,62%	3	1,11%	2	1,37%
C.3. Service Delivery	10	2,07%	1	0,37%	1	0,68%
C.4. Problem Management	19	3,94%	19	7,04%	11	7,53%
C.5. Systems Management	23	4,77%	19	7,04%	11	7,53%
D.1. Information Security Strategy Development	17	3,53%	13	4,81%	5	3,42%
D.2. Quality Strategy Development	5	1,04%	0	0,0%	1	0,68%
D.3. Education and Training Provision	0	0,0%	3	1,11%	3	2,05%
D.4. Purchasing	0	0,0%	1	0,37%	0	0,0%
D.5. Sales Development	0	0,0%	0	0,0%	0	0,0%
D.6. Digital Marketing	0	0,0%	0	0,0%	0	0,0%
D.7. Science and Analysis	22	4,56%	11	4,07%	5	3,42%
D.8. Contract Management	0	0,0%	1	0,37%	0	0,0%
D.9. Personnel Development	0	0,0%	2	0,74%	1	0,68%
D.10. Information and Knowledge Management	2	0,41%	3	1,11%	2	1,37%

Co-funded by the European Union

D.11. Needs Identification	12	2,49%	0	0,0%	1	0,68%
D.12. Security Consulting	18	3,73%	4	1,48%	2	1,37%
E.1. Forecast Development	5	1,04%	0	0,0%	0	0,0%
E.2. Project and Portfolio Management	3	0,62%	4	1,48%	0	0,0%
E.3. Risk Management	31	6,43%	27	10,00%	14	9,59%
E.4. Relationship Management	13	2,70%	4	1,48%	2	1,37%
E.5. Process Improvement	9	1,87%	1	0,37%	2	1,37%
E.6. Quality Management and Compliance	23	4,77%	16	5,93%	12	8,22%
E.7. Business Change Management	10	2,07%	2	0,74%	1	0,68%
E.8. Information Security Management	55	11,41%	40	14,81%	19	13,01%
E.9. Information Systems Governance	17	3,53%	14	5,19%	8	5,48%

Table 31. The Netherlands - Competences in comparison to (percentual) education form: class, online or hybrid

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				9	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/ Service Planning		0	0	0	
A.5. Architecture Design			10	1	0
A.6. Application/ Product Design	0	2	10		
A.7. Technology Trend Monitoring			9	6	0
A.8. Sustainability Management			5	0	
A.9. Innovating				1	0
A.10. User Experience		0	9	0	
B.1. Application/ Product Development	1	4	12		
B.2. Component Integration		4	5	0	
B.3. Testing	0	1	7	0	
B.4. Solution Deployment	1	5	5		
B.5. Documentation Production	0	1	7		
B.6. ICT Systems Engineering			7	3	
C.1. User Support	1	3	0		
C.2. Change Support		3	0		
C.3. Service Delivery	0	3	6		
C.4. Problem Management		3	2	1	
C.5. Systems Management	1	3	5		
D.1. Information Security Strategy Development				2	0
D.2. Quality Strategy Development				5	0
D.3. Education and Training Provision		0	0		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	

Co-funded by the European Union

D.7. Science and Analysis		0	9	6	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	0	
D.10. Information and Knowledge Management			0	0	0
D.11. Needs Identification			9	1	0
D.12. Security Consulting			9	0	
E.1. Forecast Development			5	0	
E.2. Project and Portfolio Management		1	0	0	0
E.3. Risk Management		0	6	2	
E.4. Relationship Management			8	1	
E.5. Process Improvement			7	1	
E.6. Quality Management and Compliance		0	6	2	
E.7. Business Change Management			5	2	0
E.8. Information Security Management		1	12	4	
E.9. Information Systems Governance				6	0

Table 32. The Netherlands - Total education offerings according to competence and proficiency level

Education		Percentage of frequency within total number of competences	Percentage of frequency within education offerings
1	B.1. Application/ Product Development	6,37%	27,42%
2	E.8. Information Security Management	6,37%	27,42%
3	A.7. Technology Trend Monitoring	5,62%	24,19%
4	D.7. Science and Analysis	5,62%	24,19%
5	A.6. Application/ Product Design	4,49%	19,35%
6	A.5. Architecture Design	4,12%	17,74%
7	B.4. Solution Deployment	4,12%	17,74%
8	B.6. ICT Systems Engineering	3,75%	16,13%
9	D.11. Needs Identification	3,75%	16,13%
10	D.12. Security Consulting	3,75%	16,13%
11	A.1. IS and Business Strategy Alignment	3,37%	14,52%
12	A.10. User Experience	3,37%	14,52%
13	B.2. Component Integration	3,37%	14,52%
14	C.3. Service Delivery	3,37%	14,52%
15	C.5. Systems Management	3,37%	14,52%
16	E.4. Relationship Management	3,37%	14,52%
17	B.3. Testing	3,00%	12,90%
18	B.5. Documentation Production	3,00%	12,90%
19	E.3. Risk Management	3,00%	12,90%
20	E.5. Process Improvement	3,00%	12,90%
21	E.6. Quality Management and Compliance	3,00%	12,90%

Co-funded by the European Union

22	E.7. Business Change Management	2,62%	11,29%
23	C.4. Problem Management	2,25%	9,68%
24	E.9. Information Systems Governance	2,25%	9,68%
25	A.8. Sustainability Management	1,87%	8,06%
26	D.2. Quality Strategy Development	1,87%	8,06%
27	E.1. Forecast Development	1,87%	8,06%
28	C.1. User Support	1,50%	6,45%
29	C.2. Change Support	1,12%	4,84%
30	D.1. Information Security Strategy Development	0,75%	3,23%
31	A.9. Innovating	0,37%	1,61%
32	E.2. Project and Portfolio Management	0,37%	1,61%
33	A.2. Service Level Management	0,0%	0,0%
34	A.3. Business Plan Development	0,0%	0,0%
35	A.4. Product/ Service Planning	0,0%	0,0%
36	D.3. Education and Training Provision	0,0%	0,0%
37	D.4. Purchasing	0,0%	0,0%
38	D.5. Sales Development	0,0%	0,0%
39	D.6. Digital Marketing	0,0%	0,0%
40	D.8. Contract Management	0,0%	0,0%
41	D.9. Personnel Development	0,0%	0,0%
42	D.10. Information and Knowledge Management	0,0%	0,0%

Table 33. The Netherlands - Competences from education offerings according to percentual frequency

Competence / Proficiency level	e1	e2	e3	e4	e5
A.1. IS and Business Strategy Alignment				4	3
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/ Service Planning		0	0	0	
A.5. Architecture Design			4	3	1
A.6. Application/ Product Design	0	0	0		
A.7. Technology Trend Monitoring			9	0	3
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		0	0	0	
B.1. Application/ Product Development	0	1	1		
B.2. Component Integration		1	3	0	
B.3. Testing	0	7	7	4	
B.4. Solution Deployment	0	2	5		
B.5. Documentation Production	0	2	6		
B.6. ICT Systems Engineering			3	2	
C.1. User Support	0	0	0		

Co-funded by the European Union

C.2. Change Support		1	2		
C.3. Service Delivery	0	2	0		
C.4. Problem Management		1	13	5	
C.5. Systems Management	0	0	14		
D.1. Information Security Strategy Development				11	3
D.2. Quality Strategy Development				1	0
D.3. Education and Training Provision		0	3		
D.4. Purchasing		0	1	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		1	7	5	0
D.8. Contract Management		0	0	1	
D.9. Personnel Development		1	0	0	
D.10. Information and Knowledge Management			0	1	0
D.11. Needs Identification			1	1	1
D.12. Security Consulting			7	3	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	1	1	0
E.3. Risk Management		4	15	8	
E.4. Relationship Management			3	1	
E.5. Process Improvement			1	3	
E.6. Quality Management and Compliance		2	13	3	
E.7. Business Change Management			3	1	0
E.8. Information Security Management		6	13	15	
E.9. Information Systems Governance				8	5

Table 34. The Netherlands - Total course offerings according to competence and proficiency level

Courses		Percentage of frequency within total number of competences	Percentage of frequency within course offerings
1	E.8. Information Security Management	12,93%	54,84%
2	E.3. Risk Management	10,27%	43,55%
3	C.4. Problem Management	7,22%	30,65%
4	B.3. Testing	6,84%	29,03%
5	E.6. Quality Management and Compliance	6,84%	29,03%
6	C.5. Systems Management	5,32%	22,58%
7	D.1. Information Security Strategy Development	5,32%	22,58%
8	D.7. Science and Analysis	4,94%	20,97%
9	E.9. Information Systems Governance	4,94%	20,97%
10	A.7. Technology Trend Monitoring	4,56%	19,35%
11	D.12. Security Consulting	3,80%	16,13%
12	A.5. Architecture Design	3,04%	12,90%

Co-funded by the European Union

13	B.5. Documentation Production	3,04%	12,90%
14	A.1. IS and Business Strategy Alignment	2,66%	11,29%
15	B.4. Solution Deployment	2,66%	11,29%
16	B.6. ICT Systems Engineering	1,90%	8,06%
17	B.2. Component Integration	1,52%	6,45%
18	E.4. Relationship Management	1,52%	6,45%
19	E.5. Process Improvement	1,52%	6,45%
20	E.7. Business Change Management	1,52%	6,45%
21	C.2. Change Support	1,14%	4,84%
22	D.3. Education and Training Provision	1,14%	4,84%
23	D.11. Needs Identification	1,14%	4,84%
24	B.1. Application/ Product Development	0,76%	3,23%
25	C.3. Service Delivery	0,76%	3,23%
26	E.2. Project and Portfolio Management	0,76%	3,23%
27	D.2. Quality Strategy Development	0,38%	1,61%
28	D.4. Purchasing	0,38%	1,61%
29	D.8. Contract Management	0,38%	1,61%
30	D.9. Personnel Development	0,38%	1,61%
31	D.10. Information and Knowledge Management	0,38%	1,61%
32	A.2. Service Level Management	0,00%	0,00%
33	A.3. Business Plan Development	0,00%	0,00%
34	A.4. Product/ Service Planning	0,00%	0,00%
35	A.6. Application/ Product Design	0,00%	0,00%
36	A.8. Sustainability Management	0,00%	0,00%
37	A.9. Innovating	0,00%	0,00%
38	A.10. User Experience	0,00%	0,00%
39	C.1. User Support	0,00%	0,00%
40	D.5. Sales Development	0,00%	0,00%
41	D.6. Digital Marketing	0,00%	0,00%
42	E.1. Forecast Development	0,00%	0,00%

Table 35. The Netherlands - Competences from course offerings according to percentual frequency

Competence / Proficiency level	e1	e2	e3	e4	e5
A.1. IS and Business Strategy Alignment				3	1
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	2
A.4. Product/ Service Planning		1	0	0	
A.5. Architecture Design			1	5	5
A.6. Application/ Product Design	0	0	3		
A.7. Technology Trend Monitoring			0	0	3
A.8. Sustainability Management			0	0	

Co-funded by the European Union

A.9. Innovating				0	2
A.10. User Experience		0	0	0	
B.1. Application/ Product Development	0	1	3		
B.2. Component Integration		1	0	3	
B.3. Testing	2	2	10	2	
B.4. Solution Deployment	0	0	6		
B.5. Documentation Production	0	0	2		
B.6. ICT Systems Engineering			5	8	
C.1. User Support	0	0	0		
C.2. Change Support		0	2		
C.3. Service Delivery	0	0	0		
C.4. Problem Management		1	7	6	
C.5. Systems Management	2	2	8		
D.1. Information Security Strategy Development				7	3
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		0	3		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		1	3	2	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	2	
D.10. Information and Knowledge Management			1	3	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			2	0	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	0	0	3
E.3. Risk Management		3	12	10	
E.4. Relationship Management			0	4	
E.5. Process Improvement			0	0	
E.6. Quality Management and Compliance		3	8	5	
E.7. Business Change Management			0	0	2
E.8. Information Security Management		15	10	16	
E.9. Information Systems Governance				7	4

Table 36. The Netherlands - Total training offerings according to competence and proficiency level

Trainings		Percentage of frequency within total number of competences	Percentage of frequency within trainings
1	E.8. Information Security Management	17,98%	73,21%
2	E.3. Risk Management	10,96%	44,64%
3	B.3. Testing	7,02%	28,57%

Co-funded by the European Union

4	E.6. Quality Management and Compliance	7,02%	28,57%
5	C.4. Problem Management	6,14%	25,00%
6	B.6. ICT Systems Engineering	5,70%	23,21%
7	C.5. System Management	5,26%	21,43%
8	A.5. Architecture Design	4,82%	19,64%
9	E.9. Information Systems Governance	4,82%	19,64%
10	D.1. Information Security Strategy Development	4,39%	17,86%
11	B.4. Solution Deployment	2,63%	10,71%
12	D.7. Science and Analysis	2,63%	10,71%
13	A.1. IS and Business Strategy Alignment	1,75%	7,14%
14	B.1. Application/ Product Development	1,75%	7,14%
15	B.2. Component Integration	1,75%	7,14%
16	D.10. Information and Knowledge Management	1,75%	7,14%
17	E.4. Relationship Management	1,75%	7,14%
18	A.6. Application/ Product Design	1,32%	5,36%
19	A.7. Technology Trend Monitoring	1,32%	5,36%
20	D.3. Education and Training Provision	1,32%	5,36%
21	E.2. Project and Portfolio Management	1,32%	5,36%
22	A.3. Business Plan Development	0,88%	3,57%
23	A.9. Innovating	0,88%	3,57%
24	B.5. Documentation Production	0,88%	3,57%
25	C.2. Change Support	0,88%	3,57%
26	D.9. Personnel Development	0,88%	3,57%
27	D.12. Security Consulting	0,88%	3,57%
28	E.7. Business Change Management	0,88%	3,57%
29	A.4. Product/ Service Planning	0,44%	1,79%
30	A.2. Service Level Management	0,00%	0,00%
31	A.8. Sustainability Management	0,00%	0,00%
32	A.10. User Experience	0,00%	0,00%
33	C.1. User Support	0,00%	0,00%
34	C.3. Service Delivery	0,00%	0,00%
35	D.2. Quality Strategy Development	0,00%	0,00%
36	D.4. Purchasing	0,00%	0,00%
37	D.5. Sales Development	0,00%	0,00%
38	D.6. Digital Marketing	0,00%	0,00%
39	D.8. Contract Management	0,00%	0,00%
40	D.11. Needs Identification	0,00%	0,00%
41	E.1. Forecast Development	0,00%	0,00%
42	E.5. Process Improvement	0,00%	0,00%

Table 37. The Netherlands - Competences from training offerings according to percentual frequency

Co-funded by the European Union

	ECSF Role	%match	St.Dev.	#No1	#No2	#No3
1	Cyber Threat Intelligence Specialist	4,50%	8,35%	22	9	2
2	Cybersecurity Risk Manager	3,57%	9,22%	17	3	0
3	Cybersecurity Researcher	1,09%	4,54%	1	5	2
4	Penetration Tester	0,82%	3,96%	2	1	2
5	Cyber Incident Responder	0,82%	3,96%	6	0	0
6	Cybersecurity Educator	0,68%	4,71%	3	0	0
7	Digital Forensics Investigator	0,51%	3,54%	1	2	0
8	Cyber, Legal, Policy & Compliance Officer	0,34%	2,90%	0	2	0
9	Chief Information Security Officer (CISO)	0,00%	0,00%	0	0	0
10	Cybersecurity Architect	0,00%	0,00%	0	0	0
11	Cybersecurity Auditor	0,00%	0,00%	0	0	0
12	Cybersecurity Implementer	0,00%	0,00%	0	0	0

Table 38. The Netherlands - ECSF Roles, average, standard deviation and top 3 education offerings

Co-funded by the European Union

Education Tables – Greece

Competence / Proficiency level	e1	e2	e3	e4	e5
A.1. IS and Business Strategy Alignment				8	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/ Service Planning		0	0	0	
A.5. Architecture Design			9	0	10
A.6. Application/ Product Design	0	0	19		
A.7. Technology Trend Monitoring			11	16	2
A.8. Sustainability Management			0	0	
A.9. Innovating				0	10
A.10. User Experience		0	0	0	
B.1. Application/ Product Development	0	0	19		
B.2. Component Integration		9	0	4	
B.3. Testing	0	0	14	18	
B.4. Solution Deployment	0	4	0		
B.5. Documentation Production	0	0	29		
B.6. ICT Systems Engineering			0	19	
C.1. User Support	0	0	0		
C.2. Change Support		0	0		
C.3. Service Delivery	0	0	0		
C.4. Problem Management		0	2	9	
C.5. Systems Management	0	0	0		
D.1. Information Security Strategy Development				4	18
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		0	2		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		0	0	12	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	2	0	
D.10. Information and Knowledge Management			2	2	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			24	23	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	0	0	0
E.3. Risk Management		0	6	27	
E.4. Relationship Management			2	0	
E.5. Process Improvement			3	0	
E.6. Quality Management and Compliance		0	0	8	

Co-funded by the European Union

E.7. Business Change Management			0	3	0
E.8. Information Security Management		0	4	25	
E.9. Information Systems Governance				5	10

Table 39. Greece – Total training, course and education market supply according to competence and proficiency level

	Trainings, Courses, Education	Percentage of frequency within total number of competences	Percentage of frequency within education items
1	D.12. Security Consulting	11,55%	100,00%
2	E.3. Risk Management	8,11%	70,21%
3	B.3. Testing	7,86%	68,09%
4	D.1. Information Security Strategy Development	7,62%	65,96%
5	A.7. Technology Trend Monitoring	7,13%	61,70%
6	B.5. Documentation Production	7,13%	61,70%
7	E.8. Information Security Management	7,13%	61,70%
8	A.5. Architecture Design	5,65%	48,94%
9	A.6. Application/Product Design	4,67%	40,43%
10	B.1. Application/Product Development	4,67%	40,43%
11	B.6. ICT Systems Engineering	4,67%	40,43%
12	E.9. Information Systems Governance	3,69%	31,91%
13	B.2. Component Integration	3,19%	27,66%
14	D.7. Science and Analysis	2,95%	25,53%
15	C.4. Problem Management	2,70%	23,40%
16	A.9. Innovating	2,46%	21,28%
17	A.1. IS and Business Strategy Alignment	1,97%	17,02%
18	E.6. Quality Management and Compliance	1,97%	17,02%
19	B.4. Solution Deployment	0,98%	8,51%
20	D.10. Information and Knowledge Management	0,98%	8,51%
21	E.5. Process Improvement	0,74%	6,38%
22	E.7. Business Change Management	0,74%	6,38%
23	D.3. Education and Training Provision	0,49%	4,26%
24	D.9. Personnel Development	0,49%	4,26%
25	E.4. Relationship Management	0,49%	4,26%
26	A.2. Service Level Management	0,00%	0,00%
27	A.3. Business Plan Development	0,00%	0,00%
28	A.4. Product/Service Planning	0,00%	0,00%
29	A.8. Sustainability Management	0,00%	0,00%
30	A.10. User Experience	0,00%	0,00%
31	C.1. User Support	0,00%	0,00%
32	C.2. Change Support	0,00%	0,00%

Co-funded by the European Union

33	C.3. Service Delivery	0,00%	0,00%
34	C.5. Systems Management	0,00%	0,00%
35	D.2. Quality Strategy Development	0,00%	0,00%
36	D.4. Purchasing	0,00%	0,00%
37	D.5. Sales Development	0,00%	0,00%
38	D.6. Digital Marketing	0,00%	0,00%
39	D.8. Contract Management	0,00%	0,00%
40	D.11. Needs Identification	0,00%	0,00%
41	E.1. Forecast Development	0,00%	0,00%
42	E.2. Project and Portfolio Management	0,00%	0,00%

Table 40. Greece - Competences from education, training and course descriptions according to percentual frequency

Class/online/hybrid	Class	Class %	Online	Online %	Hybrid	Hybrid %
A.1. IS and Business Strategy Alignment	1	1,35%	4	2,92%	3	1,96%
A.2. Service Level Management	0	0,00%	0	0,00%	0	0,00%
A.3. Business Plan Development	0	0,00%	0	0,00%	0	0,00%
A.4. Product/Service Planning	0	0,00%	0	0,00%	0	0,00%
A.5. Architecture Design	5	6,76%	9	6,57%	5	3,27%
A.6. Application/Product Design	5	6,76%	9	6,57%	5	3,27%
A.7. Technology Trend Monitoring	6	8,11%	9	6,57%	14	9,15%
A.8. Sustainability Management	0	0,00%	0	0,00%	0	0,00%
A.9. Innovating	2	2,70%	1	0,73%	7	4,58%
A.10. User Experience	0	0,00%	0	0,00%	0	0,00%
B.1. Application/Product Development	5	6,76%	9	6,57%	5	3,27%
B.2. Component Integration	3	4,05%	6	4,38%	4	2,61%
B.3. Testing	7	9,46%	17	12,41%	8	5,23%
B.4. Solution Deployment	0	0,00%	2	1,46%	2	1,31%
B.5. Documentation Production	6	8,11%	10	7,30%	13	8,50%
B.6. ICT Systems Engineering	5	6,76%	9	6,57%	5	3,27%
C.1. User Support	0	0,00%	0	0,00%	0	0,00%
C.2. Change Support	0	0,00%	0	0,00%	0	0,00%
C.3. Service Delivery	0	0,00%	0	0,00%	0	0,00%
C.4. Problem Management	3	4,05%	5	3,65%	3	1,96%
C.5. Systems Management	0	0,00%	0	0,00%	0	0,00%
D.1. Information Security Strategy Development	3	4,05%	7	5,11%	12	7,84%
D.2. Quality Strategy Development	0	0,00%	0	0,00%	0	0,00%
D.3. Education and Training Provision	0	0,00%	1	0,73%	1	0,65%
D.4. Purchasing	0	0,00%	0	0,00%	0	0,00%
D.5. Sales Development	0	0,00%	0	0,00%	0	0,00%
D.6. Digital Marketing	0	0,00%	0	0,00%	0	0,00%
D.7. Science and Analysis	2	2,70%	3	2,19%	7	4,58%
D.8. Contract Management	0	0,00%	0	0,00%	0	0,00%

Co-funded by the European Union

D.9. Personnel Development	0	0,00%	1	0,73%	1	0,65%
D.10. Information and Knowledge Management	0	0,00%	3	2,19%	1	0,65%
D.11. Needs Identification	0	0,00%	0	0,00%	0	0,00%
D.12. Security Consulting	10	13,51%	21	15,33%	3	1,96%
E.1. Forecast Development	0	0,00%	0	0,00%	0	0,00%
E.2. Project and Portfolio Management	0	0,00%	0	0,00%	0	0,00%
E.3. Risk Management	5	6,76%	7	5,11%	0	0,00%
E.4. Relationship Management	0	0,00%	0	0,00%	5	3,27%
E.5. Process Improvement	1	1,35%	0	0,00%	5	3,27%
E.6. Quality Management and Compliance	0	0,00%	0	0,00%	14	9,15%
E.7. Business Change Management	1	1,35%	0	0,00%	0	0,00%
E.8. Information Security Management	3	4,05%	1	0,73%	7	4,58%
E.9. Information Systems Governance	1	1,35%	3	2,19%	0	0,00%

Table 41. Greece - Competences in comparison to (percentual) education form: class, online or hybrid

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				2	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/Service Planning		0	0	0	
A.5. Architecture Design			1	0	5
A.6. Application/Product Design	0	0	6		
A.7. Technology Trend Monitoring			6	12	1
A.8. Sustainability Management			0	0	
A.9. Innovating				0	9
A.10. User Experience		0	0	0	
B.1. Application/Product Development	0	0	6		
B.2. Component Integration		4	0	2	
B.3. Testing	0	0	2	9	
B.4. Solution Deployment	0	2	0		
B.5. Documentation Production	0	0	17		
B.6. ICT Systems Engineering			0	6	
C.1. User Support	0	0	0		
C.2. Change Support		0	0		
C.3. Service Delivery	0	0	0		
C.4. Problem Management		0	1	4	
C.5. Systems Management	0	0	0		
D.1. Information Security Strategy Development				1	13
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		0	0		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	

Co-funded by the European Union

D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		0	0	9	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	0	
D.10. Information and Knowledge Management			1	0	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			13	8	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	0	0	0
E.3. Risk Management		0	3	16	
E.4. Relationship Management			0	0	
E.5. Process Improvement			1	0	
E.6. Quality Management and Compliance		0	0	4	
E.7. Business Change Management			0	1	0
E.8. Information Security Management		0	1	15	
E.9. Information Systems Governance				1	5

Table 42. Greece - Total education offerings according to competence and proficiency level

Education		Percentage of frequency within total number of competences	Percentage of frequency within education offerings
1	D.9. Personnel Development	11,23%	100,00%
2	E.8. Information Security Management	10,16%	90,48%
3	D.12. Security Consulting	10,16%	90,48%
4	A.9. Innovating	9,09%	80,95%
5	E.6. Quality Management and Compliance	8,56%	76,19%
6	C.1. User Support	7,49%	66,67%
7	A.7. Technology Trend Monitoring	5,88%	52,38%
8	A.2. Service Level Management	4,81%	42,86%
9	D.3. Education and Training Provision	4,81%	42,86%
10	D.1. Information Security Strategy Development	3,21%	28,57%
11	D.7. Science and Analysis	3,21%	28,57%
12	A.4. Product/Service Planning	3,21%	28,57%
13	A.6. Application/Product Design	3,21%	28,57%
14	A.10. User Experience	3,21%	28,57%
15	E.7. Business Change Management	3,21%	28,57%
16	B.4. Solution Deployment	2,67%	23,81%
17	E.4. Relationship Management	2,14%	19,05%
18	E.3. Risk Management	1,07%	9,52%
19	A.8. Sustainability Management	1,07%	9,52%
20	D.6. Digital Marketing	0,53%	4,76%
21	E.2. Project and Portfolio Management	0,53%	4,76%

Co-funded by the European Union

22	E.5. Process Improvement	0,53%	4,76%
23	B.6. ICT Systems Engineering	0,00%	0,00%
24	E.9. Information Systems Governance	0,00%	0,00%
25	A.5. Architecture Design	0,00%	0,00%
26	A.1. IS and Business Strategy Alignment	0,00%	0,00%
27	A.3. Business Plan Development	0,00%	0,00%
28	B.1. Application/Product Development	0,00%	0,00%
29	B.2. Component Integration	0,00%	0,00%
30	B.3. Testing	0,00%	0,00%
31	B.5. Documentation Production	0,00%	0,00%
32	C.2. Change Support	0,00%	0,00%
33	C.3. Service Delivery	0,00%	0,00%
34	C.4. Problem Management	0,00%	0,00%
35	C.5. Systems Management	0,00%	0,00%
36	D.2. Quality Strategy Development	0,00%	0,00%
37	D.4. Purchasing	0,00%	0,00%
38	D.5. Sales Development	0,00%	0,00%
39	D.8. Contract Management	0,00%	0,00%
40	D.10. Information and Knowledge Management	0,00%	0,00%
41	D.11. Needs Identification	0,00%	0,00%
42	E.1. Forecast Development	0,00%	0,00%

Table 43. Greece - Competences from education offerings according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				6	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/Service Planning		0	0	0	
A.5. Architecture Design			8	0	5
A.6. Application/Product Design	0	0	13		
A.7. Technology Trend Monitoring			5	4	1
A.8. Sustainability Management			0	0	
A.9. Innovating				0	1
A.10. User Experience		0	0	0	
B.1. Application/Product Development	0	0	13		
B.2. Component Integration		5	0	2	
B.3. Testing	0	0	12	9	
B.4. Solution Deployment	0	2	0		
B.5. Documentation Production	0	0	12		
B.6. ICT Systems Engineering			0	13	

Co-funded by the European Union

C.1. User Support	0	0	0		
C.2. Change Support		0	0		
C.3. Service Delivery	0	0	0		
C.4. Problem Management		0	1	5	
C.5. Systems Management	0	0	0		
D.1. Information Security Strategy Development				3	5
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		0	2		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		0	0	3	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	2	0	
D.10. Information and Knowledge Management			1	2	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			11	15	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	0	0	0
E.3. Risk Management		0	3	11	
E.4. Relationship Management			2	0	
E.5. Process Improvement			2	0	
E.6. Quality Management and Compliance		0	0	4	
E.7. Business Change Management			0	2	0
E.8. Information Security Management		0	3	10	
E.9. Information Systems Governance				4	5

Table 44. Greece - Total course offerings according to competence and proficiency level

Courses		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	D.12. Security Consulting	12,56%	100,00%
2	B.3. Testing	10,14%	80,77%
3	E.3. Risk Management	6,76%	53,85%
4	A.5. Architecture Design	6,28%	50,00%
5	A.6. Application/Product Design	6,28%	50,00%
6	B.1. Application/Product Development	6,28%	50,00%
7	B.6. ICT Systems Engineering	6,28%	50,00%
8	E.8. Information Security Management	6,28%	50,00%
9	B.5. Documentation Production	5,80%	46,15%
10	A.7. Technology Trend Monitoring	4,83%	38,46%

Co-funded by the European Union

11	E.9. Information Systems Governance	4,35%	34,62%
12	D.1. Information Security Strategy Development	3,86%	30,77%
13	B.2. Component Integration	3,38%	26,92%
14	A.1. IS and Business Strategy Alignment	2,90%	23,08%
15	C.4. Problem Management	2,90%	23,08%
16	E.6. Quality Management and Compliance	1,93%	15,38%
17	D.7. Science and Analysis	1,45%	11,54%
18	D.10. Information and Knowledge Management	1,45%	11,54%
19	B.4. Solution Deployment	0,97%	7,69%
20	D.3. Education and Training Provision	0,97%	7,69%
21	D.9. Personnel Development	0,97%	7,69%
22	E.4. Relationship Management	0,97%	7,69%
23	E.5. Process Improvement	0,97%	7,69%
24	E.7. Business Change Management	0,97%	7,69%
25	A.9. Innovating	0,48%	3,85%
26	A.2. Service Level Management	0,00%	0,00%
27	A.3. Business Plan Development	0,00%	0,00%
28	A.4. Product/Service Planning	0,00%	0,00%
29	A.8. Sustainability Management	0,00%	0,00%
30	A.10. User Experience	0,00%	0,00%
31	C.1. User Support	0,00%	0,00%
32	C.2. Change Support	0,00%	0,00%
33	C.3. Service Delivery	0,00%	0,00%
34	C.5. Systems Management	0,00%	0,00%
35	D.2. Quality Strategy Development	0,00%	0,00%
36	D.4. Purchasing	0,00%	0,00%
37	D.5. Sales Development	0,00%	0,00%
38	D.6. Digital Marketing	0,00%	0,00%
39	D.8. Contract Management	0,00%	0,00%
40	D.11. Needs Identification	0,00%	0,00%
41	E.1. Forecast Development	0,00%	0,00%
42	E.2. Project and Portfolio Management	0,00%	0,00%

Table 45. Greece - Competences from course offerings according to percentual frequency

	ECSF Role	%match	St.Dev.	#No1	#No2	#No3
1	Penetration Tester	7,31%	9,63%	8	11	0
2	Cybersecurity Risk Manager	5,29%	10,21%	11	0	0
3	Cyber Threat Intelligence Specialist	2,31%	6,39%	4	2	0
4	Cybersecurity Researcher	0,77%	3,85%	1	1	0

Co-funded by the European Union

5	Chief Information Security Officer (CISO)	0,00%	0,00%	0	0	0
6	Cyber Incident Responder	0,00%	0,00%	0	0	0
7	Cyber, Legal, Policy & Compliance Officer	0,00%	0,00%	0	0	0
8	Cybersecurity Architect	0,00%	0,00%	0	0	0
9	Cybersecurity Auditor	0,00%	0,00%	0	0	0
10	Cybersecurity Educator	0,00%	0,00%	0	0	0
11	Cybersecurity Implementer	0,00%	0,00%	0	0	0
12	Digital Forensics Investigator	0,00%	0,00%	0	0	0

Table 46. Greece - ECSF Roles, average, standard deviation and top 3 education offerings

Co-funded by the European Union

Education Tables – Cyprus

Competence / Proficiency level	e1	e2	e3	e4	e5
A.1. IS and Business Strategy Alignment				0	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/ Service Planning		0	0	0	
A.5. Architecture Design			0	1	0
A.6. Application/ Product Design	0	0	0		
A.7. Technology Trend Monitoring			5	0	0
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		0	0	0	
B.1. Application/ Product Development	1	0	0		
B.2. Component Integration		0	0	0	
B.3. Testing	1	0	0	0	
B.4. Solution Deployment	0	0	0		
B.5. Documentation Production	1	0	0		
B.6. ICT Systems Engineering			3	0	
C.1. User Support	1	0	0		
C.2. Change Support		1	1		
C.3. Service Delivery	0	0	0		
C.4. Problem Management		1	0	0	
C.5. Systems Management	0	0	0		
D.1. Information Security Strategy Development				3	0
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		0	0		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		1	1	0	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	0	
D.10. Information and Knowledge Management			0	0	0
D.11. Needs Identification			0	0	0
D.12. Security Consulting			0	0	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		0	0	0	0
E.3. Risk Management		6	3	0	
E.4. Relationship Management			0	0	
E.5. Process Improvement			0	0	
E.6. Quality Management and Compliance		0	0	0	

Co-funded by the European Union

E.7. Business Change Management			0	0	0
E.8. Information Security Management		1	1	0	
E.9. Information Systems Governance				5	0

Table 47. Cyprus – Total training, course and education market supply according to competence and proficiency level

Trainings, Courses, Education		Percentage of frequency within total number of competences	Percentage of frequency within education items
1	E.3. Risk Management	25,71%	69,23%
2	A.7. Technology Trend Monitoring	14,29%	38,46%
3	E.9. Information Systems Governance	14,29%	38,46%
4	B.6. ICT Systems Engineering	8,57%	23,08%
5	D.1. Information Security Strategy Development	8,57%	23,08%
6	D.7. Science and Analysis	5,71%	15,38%
7	E.8. Information Security Management	5,71%	15,38%
8	A.5. Architecture Design	2,86%	7,69%
9	B.1. Application/ Product Development	2,86%	7,69%
10	B.3. Testing	2,86%	7,69%
11	B.5. Documentation Production	2,86%	7,69%
12	C.1. User Support	2,86%	7,69%
13	C.4. Problem Management	2,86%	7,69%
14	A.1. IS and Business Strategy Alignment	0,00%	0,00%
15	A.2. Service Level Management	0,00%	0,00%
16	A.3. Business Plan Development	0,00%	0,00%
17	A.4. Product/ Service Planning	0,00%	0,00%
18	A.6. Application/ Product Design	0,00%	0,00%
19	A.8. Sustainability Management	0,00%	0,00%
20	A.9. Innovating	0,00%	0,00%
21	A.10. User Experience	0,00%	0,00%
22	B.2. Component Integration	0,00%	0,00%
23	B.4. Solution Deployment	0,00%	0,00%
24	C.2. Change Support	0,00%	0,00%
25	C.3. Service Delivery	0,00%	0,00%
26	C.5. Systems Management	0,00%	0,00%
27	D.2. Quality Strategy Development	0,00%	0,00%
28	D.3. Education and Training Provision	0,00%	0,00%
29	D.4. Purchasing	0,00%	0,00%
30	D.5. Sales Development	0,00%	0,00%
31	D.6. Digital Marketing	0,00%	0,00%
32	D.8. Contract Management	0,00%	0,00%

Co-funded by the European Union

33	D.9. Personnel Development	0,00%	0,00%
34	D.10. Information and Knowledge Management	0,00%	0,00%
35	D.11. Needs Identification	0,00%	0,00%
36	D.12. Security Consulting	0,00%	0,00%
37	E.1. Forecast Development	0,00%	0,00%
38	E.2. Project and Portfolio Management	0,00%	0,00%
39	E.4. Relationship Management	0,00%	0,00%
40	E.5. Process Improvement	0,00%	0,00%
41	E.6. Quality Management and Compliance	0,00%	0,00%
42	E.7. Business Change Management	0,00%	0,00%

Table 48. Cyprus - Competences from education, training and course descriptions according to percentual frequency

Competence / Proficiency level	Class	Class %	Online	Online %	Hybrid	Hybrid %
A.5. Architecture Design	1	12,50%	0	0%	0	0%
A.7. Technology Trend Monitoring	0	0%	5	20%	0	0%
B.1. Application/Product Development	0	0%	1	4,00%	0	0%
B.3. Testing	0	0%	1	4,00%	0	0%
B.5. Documentation Production	0	0%	1	4,00%	0	0%
B.6. ICT Systems Engineering	1	12,50%	1	4,00%	1	50,0%
C.1. User Support	0	0%	1	4,00%	0	0%
C.4. Problem Management	0	0%	1	4,00%	0	0%
D.1. Information Security Strategy Dev.	1	12,50%	2	8,00%	0	0%
D.7. Science and Analysis	1	12,50%	1	4,00%	0	0%
E.3. Risk Management	2	25%	7	28,00%	0	0%
E.8. Information Security Management	1	12,50%	1	4,00%	0	0%
E.9. Information Systems Governance	1	12,50%	3	12,00%	1	50,0%

Table 49. Cyprus - Competences in comparison to (percentual) education form: class, online or hybrid

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.5. Architecture Design	0	0	0	1	0
B.6. ICT Systems Engineering	0	0	2	0	0
D.1. Information Security Strategy Development	0	0	1	0	0
D.7. Science and Analysis	0	0	1	0	0
E.3. Risk Management	0	0	3	0	0
E.8. Information Security Management	0	0	1	0	0
E.9. Information Systems Governance	0	0	2	0	0

Table 50. Cyprus - Total education offerings according to competence and proficiency level

Co-funded by the European Union

Education		Percentage of frequency within total number of competences	Percentage of frequency within vacancies
1	E.3. Risk Management	27,27%	75,00%
2	B.6. ICT Systems Engineering	18,18%	50,00%
3	E.9. Information Systems Governance	18,18%	50,00%
4	D.1. Information Security Strategy Development	9,09%	25,00%
5	D.7. Science and Analysis	9,09%	25,00%
6	E.8. Information Security Management	9,09%	25,00%
7	A.5. Architecture Design	9,09%	25,00%

Table 51. Cyprus - Competences from education offerings according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.7. Technology Trend Monitoring	0	0	5	0	0
B.1. Application/Product Development	1	0	0	0	0
B.3. Testing	1	0	0	0	0
B.5. Documentation Production	1	0	0	0	0
B.6. ICT Systems Engineering	0	0	1	0	0
C.1. User Support	1	0	0	0	0
C.4. Problem Management	1	0	0	0	0
D.1. Information Security Strategy Development	0	0	0	2	0
D.7. Science and Analysis	0	1	0	0	0
E.3. Risk Management	0	6	0	0	0
E.8. Information Security Management	0	1	0	0	0
E.9. Information Systems Governance	0	0	0	3	0

Table 52. Cyprus - Total training offerings according to competence and proficiency level

Trainings		Percentage of frequency within total number of competences	Within education offerings
1	E.3. Risk Management	25,00%	66,67%
2	A.7. Technology Trend Monitoring	20,83%	55,56%
3	E.9. Information Systems Governance	12,50%	33,33%
4	D.1. Information Security Strategy Development	8,33%	22,22%
5	B.1. Application/Product Development	4,17%	11,11%
6	B.3. Testing	4,17%	11,11%
7	B.5. Documentation Production	4,17%	11,11%
8	B.6. ICT Systems Engineering	4,17%	11,11%
9	C.1. User Support	4,17%	11,11%
10	C.4. Problem Management	4,17%	11,11%
11	D.7. Science and Analysis	4,17%	11,11%
12	E.8. Information Security Management	4,17%	11,11%

Table 53. Cyprus - Competences from training offerings according to percentual frequency

Co-funded by the European Union

	ECSF Role	%match	St.Dev.	#No1	#No2	#No3
1	Cyber Threat Intelligence Specialist	3,16%	7,29%	3	0	0
2	Chief Information Security Officer (CISO)	0,00%	0,00%	0	0	0
3	Cyber Incident Responder	0,00%	0,00%	0	0	0
4	Cyber, Legal, Policy & Compliance Officer	0,00%	0,00%	0	0	0
5	Cybersecurity Architect	0,00%	0,00%	0	0	0
6	Cybersecurity Auditor	0,00%	0,00%	0	0	0
7	Cybersecurity Educator	0,00%	0,00%	0	0	0
8	Cybersecurity Implementer	0,00%	0,00%	0	0	0
9	Cybersecurity Researcher	0,00%	0,00%	0	0	0
10	Cybersecurity Risk Manager	0,00%	0,00%	0	0	0
11	Digital Forensics Investigator	0,00%	0,00%	0	0	0
12	Penetration Tester	0,00%	0,00%	0	0	0

Table 54. Cyprus - ECSF Roles, average, standard deviation and top 3 education offerings

Co-funded by the European Union

Education Tables – Croatia

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				7	1
A.2. Service Level Management			1	2	
A.3. Business Plan Development			6	2	2
A.4. Product/ Service Planning		11	4	1	
A.5. Architecture Design			30	14	0
A.6. Application/ Product Design	5	17	20		
A.7. Technology Trend Monitoring			10	4	0
A.8. Sustainability Management			4	1	
A.9. Innovating				5	0
A.10. User Experience		11	7	3	
B.1. Application/ Product Development	6	14	38		
B.2. Component Integration		18	22	3	
B.3. Testing	11	8	16	6	
B.4. Solution Deployment	9	8	16		
B.5. Documentation Production	7	17	17		
B.6. ICT Systems Engineering			36	10	
C.1. User Support	8	6	4		
C.2. Change Support		2	6		
C.3. Service Delivery	1	2	2		
C.4. Problem Management		14	20	10	
C.5. Systems Management	10	20	31		
D.1. Information Security Strategy Development				7	1
D.2. Quality Strategy Development				3	0
D.3. Education and Training Provision		6	8		
D.4. Purchasing		6	0	0	
D.5. Sales Development		1	1	0	
D.6. Digital Marketing		1	1	0	
D.7. Science and Analysis		14	31	17	0
D.8. Contract Management		2	0	0	
D.9. Personnel Development		2	10	1	
D.10. Information and Knowledge Management			15	4	0
D.11. Needs Identification			21	6	0
D.12. Security Consulting			13	10	
E.1. Forecast Development			7	2	
E.2. Project and Portfolio Management		22	18	6	0
E.3. Risk Management		7	14	13	
E.4. Relationship Management			13	2	
E.5. Process Improvement			21	6	
E.6. Quality Management and Compliance		2	19	8	

Co-funded by the European Union

E.7 .Business Change Management			8	1	1
E.8. Information Security Management		20	24	13	
E.9. Information Systems Governance				15	3

Table 55. Croatia – Total training, course and education market supply according to competence and proficiency level

Trainings, Courses, Education		Percentage of frequency within total number of competences	Percentage of frequency within total education items
1	D.7. Science and Analysis	6,25%	67,39%
2	C.5. Systems Management	6,15%	66,30%
3	B.1. Application/Product Development	5,85%	63,04%
4	E.8. Information Security Management	5,75%	61,96%
5	B.6. ICT Systems Engineering	4,64%	50,00%
6	E.2. Project and Portfolio Management	4,64%	50,00%
7	A.5. Architecture Design	4,44%	47,83%
8	C.4. Problem Management	4,44%	47,83%
9	B.2. Component Integration	4,33%	46,74%
10	A.6. Application/Product Design	4,23%	45,65%
11	B.3. Testing	4,13%	44,57%
12	B.5. Documentation Production	4,13%	44,57%
13	E.3. Risk Management	3,43%	36,96%
14	B.4. Solution Deployment	3,33%	35,87%
15	E.6. Quality Management and Compliance	2,92%	31,52%
16	D.11. Needs Identification	2,72%	29,35%
17	E.5. Process Improvement	2,72%	29,35%
18	D.12. Security Consulting	2,32%	25,00%
19	A.10. User Experience	2,12%	22,83%
20	D.10. Information and Knowledge Management	1,92%	20,65%
21	C.1. User Support	1,81%	19,57%
22	E.9. Information Systems Governance	1,81%	19,57%
23	A.4. Product/Service Planning	1,61%	17,39%
24	E.4. Relationship Management	1,51%	16,30%
25	A.7. Technology Trend Monitoring	1,41%	15,22%
26	D.3. Education and Training Provision	1,41%	15,22%
27	D.9. Personnel Development	1,31%	14,13%
28	A.3. Business Plan Development	1,01%	10,87%
29	E.7. Business Change Management	1,01%	10,87%
30	E.1. Forecast Development	0,91%	9,78%
31	A.1. IS and Business Strategy Alignment	0,81%	8,70%
32	C.2. Change Support	0,81%	8,70%
33	D.1. Information Security Strategy Development	0,81%	8,70%
34	D.4. Purchasing	0,60%	6,52%

Co-funded by the European Union

35	A.8. Sustainability Management	0,50%	5,43%
36	A.9. Innovating	0,50%	5,43%
37	C.3. Service Delivery	0,50%	5,43%
38	A.2. Service Level Management	0,30%	3,26%
39	D.2. Quality Strategy Development	0,30%	3,26%
40	D.5. Sales Development	0,20%	2,17%
41	D.6. Digital Marketing	0,20%	2,17%
42	D.8. Contract Management	0,20%	2,17%

Table 56. Croatia - Competences from education, training and course descriptions according to percentual frequency

Class/online/hybrid	Class	Class %	Online	Online %	Hybrid	Hybrid %
A.1. IS and Business Strategy Alignment	3	0,44%	0	0,00%	4	1,92%
A.2. Service Level Management	2	0,29%	0	0,00%	0	0,00%
A.3. Business Plan Development	4	0,58%	1	0,73%	2	0,96%
A.4. Product/ Service Planning	13	1,89%	0	0,00%	1	0,48%
A.5. Architecture Design	28	4,08%	1	0,73%	12	5,77%
A.6. Application/ Product Design	29	4,22%	0	0,00%	11	5,29%
A.7. Technology Trend Monitoring	7	1,02%	1	0,73%	4	1,92%
A.8. Sustainability Management	2	0,29%	1	0,73%	0	0,00%
A.9. Innovating	2	0,29%	0	0,00%	2	0,96%
A.10. User Experience	15	2,18%	0	0,00%	3	1,44%
B.1. Application/ Product Development	41	5,97%	2	1,46%	11	5,29%
B.2. Component Integration	30	4,37%	0	0,00%	9	4,33%
B.3. Testing	37	5,39%	10	7,30%	2	0,96%
B.4. Solution Deployment	28	4,08%	4	2,92%	1	0,48%
B.5. Documentation Production	30	4,37%	6	4,38%	9	4,33%
B.6. ICT Systems Engineering	34	4,95%	6	4,38%	8	3,85%
C.1. User Support	14	2,04%	0	0,00%	4	1,92%
C.2. Change Support	5	0,73%	0	0,00%	0	0,00%
C.3. Service Delivery	2	0,29%	0	0,00%	2	0,96%
C.4. Problem Management	39	5,68%	11	8,03%	2	0,96%
C.5. Systems Management	47	6,84%	10	7,30%	12	5,77%
D.1. Information Security Strategy Development	4	0,58%	2	1,46%	3	1,44%
D.2. Quality Strategy Development	1	0,15%	0	0,00%	2	0,96%
D.3. Education and Training Provision	6	0,87%	3	2,19%	8	3,85%
D.4. Purchasing	6	0,87%	0	0,00%	0	0,00%
D.5. Sales Development	1	0,15%	0	0,00%	0	0,00%
D.6. Digital Marketing	2	0,29%	0	0,00%	0	0,00%
D.7. Science and Analysis	48	6,99%	12	8,76%	9	4,33%
D.8. Contract Management	0	0,00%	0	0,00%	2	0,96%
D.9. Personnel Development	0	0,00%	0	0,00%	10	4,81%
D.10. Information and Knowledge Management	16	2,33%	5	3,65%	0	0,00%

Co-funded by the European Union

D.11. Needs Identification	13	1,89%	1	0,73%	10	4,81%
D.12. Security Consulting	15	2,18%	11	8,03%	7	3,37%
E.1. Forecast Development	6	0,87%	2	1,46%	1	0,48%
E.2. Project and Portfolio Management	36	5,24%	7	5,11%	4	1,92%
E.3. Risk Management	24	3,49%	12	8,76%	6	2,88%
E.4. Relationship Management	4	0,58%	0	0,00%	8	3,85%
E.5. Process Improvement	18	2,62%	1	0,73%	8	3,85%
E.6. Quality Management and Compliance	18	2,62%	12	8,76%	9	4,33%
E.7. Business Change Management	5	0,73%	0	0,00%	2	0,96%
E.8. Information Security Management	43	6,26%	12	8,76%	12	5,77%
E.9. Information Systems Governance	9	1,31%	4	2,92%	8	3,85%

Table 57. Croatia - Competences in comparison to (percentual) education form: class, online or hybrid

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				7	1
A.2. Service Level Management			1	2	
A.3. Business Plan Development			6	2	2
A.4. Product/ Service Planning		11	4	1	
A.5. Architecture Design			28	13	0
A.6. Application/ Product Design	5	17	20		
A.7. Technology Trend Monitoring			10	3	0
A.8. Sustainability Management			4	1	
A.9. Innovating				5	0
A.10. User Experience		9	7	3	
B.1. Application/ Product Development	6	14	37		
B.2. Component Integration		16	21	3	
B.3. Testing	11	8	8	2	
B.4. Solution Deployment	9	8	6		
B.5. Documentation Production	7	16	9		
B.6. ICT Systems Engineering			32	6	
C.1. User Support	8	4	4		
C.2. Change Support		2	5		
C.3. Service Delivery	0	0	2		
C.4. Problem Management		13	16	2	
C.5. Systems Management	10	17	21		
D.1. Information Security Strategy Development				5	1
D.2. Quality Strategy Development				3	0
D.3. Education and Training Provision		5	6		
D.4. Purchasing		6	0	0	
D.5. Sales Development		1	1	0	
D.6. Digital Marketing		1	1	0	
D.7. Science and Analysis		8	25	15	0

Co-funded by the European Union

D.8. Contract Management		0	0	0	
D.9. Personnel Development		2	10	1	
D.10. Information and Knowledge Management			12	3	0
D.11. Needs Identification			18	5	0
D.12. Security Consulting			5	4	
E.1. Forecast Development			3	1	
E.2. Project and Portfolio Management		19	15	5	0
E.3. Risk Management		6	8	7	
E.4. Relationship Management			11	2	
E.5. Process Improvement			20	5	
E.6. Quality Management and Compliance		2	9	6	
E.7. Business Change Management			6	1	1
E.8. Information Security Management		17	17	6	
E.9. Information Systems Governance				10	1

Table 58. Croatia - Total education offerings according to competence and proficiency level

Education		Percentage of frequency within total number of competences	Percentage of frequency within education items
1	B.1. Application/Product Development	7,12%	89,06%
2	C.5. Systems Management	5,99%	75,00%
3	D.7. Science and Analysis	5,99%	75,00%
4	A.6. Application/Product Design	5,24%	65,63%
5	A.5. Architecture Design	5,12%	64,06%
6	B.2. Component Integration	4,99%	62,50%
7	E.8. Information Security Management	4,99%	62,50%
8	E.2. Project and Portfolio Management	4,87%	60,94%
9	B.6. ICT Systems Engineering	4,74%	59,38%
10	B.5. Documentation Production	4,00%	50,00%
11	C.4. Problem Management	3,87%	48,44%
12	B.3. Testing	3,62%	45,31%
13	E.5. Process Improvement	3,12%	39,06%
14	B.4. Solution Deployment	2,87%	35,94%
15	D.11. Needs Identification	2,87%	35,94%
16	E.3. Risk Management	2,62%	32,81%
17	A.10. User Experience	2,37%	29,69%
18	E.6. Quality Management and Compliance	2,12%	26,56%
19	A.4. Product/Service Planning	2,00%	25,00%
20	C.1. User Support	2,00%	25,00%
21	D.10. Information and Knowledge Management	1,87%	23,44%
22	A.7. Technology Trend Monitoring	1,62%	20,31%
23	D.9. Personnel Development	1,62%	20,31%

Co-funded by the European Union

24	E.4. Relationship Management	1,62%	20,31%
25	D.3. Education and Training Provision	1,37%	17,19%
26	E.9. Information Systems Governance	1,37%	17,19%
27	A.3. Business Plan Development	1,25%	15,63%
28	D.12. Security Consulting	1,12%	14,06%
29	A.1. IS and Business Strategy Alignment	1,00%	12,50%
30	E.7. Business Change Management	1,00%	12,50%
31	C.2. Change Support	0,87%	10,94%
32	D.1. Information Security Strategy Development	0,75%	9,38%
33	D.4. Purchasing	0,75%	9,38%
34	A.8. Sustainability Management	0,62%	7,81%
35	A.9. Innovating	0,62%	7,81%
36	E.1. Forecast Development	0,50%	6,25%
37	A.2. Service Level Management	0,37%	4,69%
38	D.2. Quality Strategy Development	0,37%	4,69%
39	C.3. Service Delivery	0,25%	3,13%
40	D.5. Sales Development	0,25%	3,13%
41	D.6. Digital Marketing	0,25%	3,13%
42	D.8. Contract Management	0,00%	0,00%

Table 59. Croatia - Competences from education offerings according to percentual frequency

Competence / Proficiency level	e-1	e-2	e-3	e-4	e-5
A.1. IS and Business Strategy Alignment				0	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/ Service Planning		0	0	0	
A.5. Architecture Design			2	1	0
A.6. Application/ Product Design	0	0	0		
A.7. Technology Trend Monitoring			0	0	0
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		0	0	0	
B.1. Application/ Product Development	0	0	1		
B.2. Component Integration		0	1	0	
B.3. Testing	0	0	6	4	
B.4. Solution Deployment	0	0	9		
B.5. Documentation Production	0	1	4		
B.6. ICT Systems Engineering			4	3	
C.1. User Support	0	0	0		
C.2. Change Support		0	1		
C.3. Service Delivery	0	1	0		

Co-funded by the European Union

C.4. Problem Management		1	2	7	
C.5. Systems Management	0	3	8		
D.1. Information Security Strategy Development				1	0
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		1	1		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		5	6	1	0
D.8. Contract Management		0	0	0	
D.9. Personnel Development		0	0	0	
D.10. Information and Knowledge Management			1	1	0
D.11. Needs Identification			1	1	0
D.12. Security Consulting			5	4	
E.1. Forecast Development			4	1	
E.2. Project and Portfolio Management		1	3	1	0
E.3. Risk Management		1	4	5	
E.4. Relationship Management			2	0	
E.5. Process Improvement			1	1	
E.6. Quality Management and Compliance		0	8	1	
E.7. Business Change Management			2	0	0
E.8. Information Security Management		3	6	5	
E.9. Information Systems Governance				2	1

Table 60. Croatia - Total course offerings according to competence and proficiency level

Courses		Percentage of frequency within total number of competences	Percentage of frequency within courses items
1	E.8. Information Security Management	10,07%	60,87%
2	D.7. Science and Analysis	8,63%	52,17%
3	C.5. Systems Management	7,91%	47,83%
4	B.3. Testing	7,19%	43,48%
5	C.4. Problem Management	7,19%	43,48%
6	E.3. Risk Management	7,19%	43,48%
7	B.4. Solution Deployment	6,47%	39,13%
8	D.12. Security Consulting	6,47%	39,13%
9	E.6. Quality Management and Compliance	6,47%	39,13%
10	B.6. ICT Systems Engineering	5,04%	30,43%
11	B.5. Documentation Production	3,60%	21,74%
12	E.1. Forecast Development	3,60%	21,74%
13	E.2. Project and Portfolio Management	3,60%	21,74%
14	A.5. Architecture Design	2,16%	13,04%

Co-funded by the European Union

15	E.9. Information Systems Governance	2,16%	13,04%
16	D.3. Education and Training Provision	1,44%	8,70%
17	D.10. Information and Knowledge Management	1,44%	8,70%
18	D.11. Needs Identification	1,44%	8,70%
19	E.4. Relationship Management	1,44%	8,70%
20	E.5. Process Improvement	1,44%	8,70%
21	E.7. Business Change Management	1,44%	8,70%
22	B.1. Application/Product Development	0,72%	4,35%
23	B.2. Component Integration	0,72%	4,35%
24	C.2. Change Support	0,72%	4,35%
25	C.3. Service Delivery	0,72%	4,35%
26	D.1. Information Security Strategy Development	0,72%	4,35%
27	A.1. IS and Business Strategy Alignment	0,00%	0,00%
28	A.2. Service Level Management	0,00%	0,00%
29	A.3. Business Plan Development	0,00%	0,00%
30	A.4. Product/Service Planning	0,00%	0,00%
31	A.6. Application/Product Design	0,00%	0,00%
32	A.7. Technology Trend Monitoring	0,00%	0,00%
33	A.8. Sustainability Management	0,00%	0,00%
34	A.9. Innovating	0,00%	0,00%
35	A.10. User Experience	0,00%	0,00%
36	C.1. User Support	0,00%	0,00%
37	D.2. Quality Strategy Development	0,00%	0,00%
38	D.4. Purchasing	0,00%	0,00%
39	D.5. Sales Development	0,00%	0,00%
40	D.6. Digital Marketing	0,00%	0,00%
41	D.8. Contract Management	0,00%	0,00%
42	D.9. Personnel Development	0,00%	0,00%

Table 61. Croatia - Competences from course offerings according to percentual frequency

Competence / proficiency level	e1	e2	e3	e4	e5
A.1. IS and Business Strategy Alignment				0	0
A.2. Service Level Management			0	0	
A.3. Business Plan Development			0	0	0
A.4. Product/ Service Planning		0	0	0	
A.5. Architecture Design			0	0	0
A.6. Application/ Product Design	0	0	0		
A.7. Technology Trend Monitoring			0	1	0
A.8. Sustainability Management			0	0	
A.9. Innovating				0	0
A.10. User Experience		2	0	0	

Co-funded by the European Union

B.1. Application/ Product Development	0	0	0		
B.2. Component Integration		2	0	0	
B.3. Testing	0	0	2	0	
B.4. Solution Deployment	0	0	1		
B.5. Documentation Production	0	0	4		
B.6. ICT Systems Engineering			0	1	
C.1. User Support	0	2	0		
C.2. Change Support		0	0		
C.3. Service Delivery	1	1	0		
C.4. Problem Management		0	2	1	
C.5. Systems Management	0	0	2		
D.1. Information Security Strategy Development				1	0
D.2. Quality Strategy Development				0	0
D.3. Education and Training Provision		0	1		
D.4. Purchasing		0	0	0	
D.5. Sales Development		0	0	0	
D.6. Digital Marketing		0	0	0	
D.7. Science and Analysis		1	0	1	0
D.8. Contract Management		2	0	0	
D.9. Personnel Development		0	0	0	
D.10. Information and Knowledge Management			2	0	0
D.11. Needs Identification			2	0	0
D.12. Security Consulting			3	2	
E.1. Forecast Development			0	0	
E.2. Project and Portfolio Management		2	0	0	0
E.3. Risk Management		0	2	1	
E.4. Relationship Management			0	0	
E.5. Process Improvement			0	0	
E.6. Quality Management and Compliance		0	2	1	
E.7. Business Change Management			0	0	0
E.8. Information Security Management		0	1	2	
E.9. Information Systems Governance				3	1

Table 62. Croatia - Total training offerings according to competence and proficiency level

Trainings		Percentage of frequency within total number of competences	Percentage of frequency within training items
1	D.12. Security Consulting	9,62%	100,00%
2	B.5. Documentation Production	7,69%	80,00%
3	E.9. Information Systems Governance	7,69%	80,00%
4	C.4. Problem Management	5,77%	60,00%
5	E.3. Risk Management	5,77%	60,00%

Co-funded by the European Union

6	E.6. Quality Management and Compliance	5,77%	60,00%
7	E.8. Information Security Management	5,77%	60,00%
8	A.10. User Experience	3,85%	40,00%
9	B.2. Component Integration	3,85%	40,00%
10	B.3. Testing	3,85%	40,00%
11	C.1. User Support	3,85%	40,00%
12	C.3. Service Delivery	3,85%	40,00%
13	C.5. Systems Management	3,85%	40,00%
14	D.7. Science and Analysis	3,85%	40,00%
15	D.8. Contract Management	3,85%	40,00%
16	D.10. Information and Knowledge Management	3,85%	40,00%
17	D.11. Needs Identification	3,85%	40,00%
18	E.2. Project and Portfolio Management	3,85%	40,00%
19	A.7. Technology Trend Monitoring	1,92%	20,00%
20	B.4. Solution Deployment	1,92%	20,00%
21	B.6. ICT Systems Engineering	1,92%	20,00%
22	D.1. Information Security Strategy Development	1,92%	20,00%
23	D.3. Education and Training Provision	1,92%	20,00%
24	A.1. IS and Business Strategy Alignment	0,00%	0,00%
25	A.2. Service Level Management	0,00%	0,00%
26	A.3. Business Plan Development	0,00%	0,00%
27	A.4. Product/Service Planning	0,00%	0,00%
28	A.5. Architecture Design	0,00%	0,00%
29	A.6. Application/Product Design	0,00%	0,00%
30	A.8. Sustainability Management	0,00%	0,00%
31	A.9. Innovating	0,00%	0,00%
32	B.1. Application/Product Development	0,00%	0,00%
33	C.2. Change Support	0,00%	0,00%
34	D.2. Quality Strategy Development	0,00%	0,00%
35	D.4. Purchasing	0,00%	0,00%
36	D.5. Sales Development	0,00%	0,00%
37	D.6. Digital Marketing	0,00%	0,00%
38	D.9. Personnel Development	0,00%	0,00%
39	E.1. Forecast Development	0,00%	0,00%
40	E.4. Relationship Management	0,00%	0,00%
41	E.5. Process Improvement	0,00%	0,00%
42	E.7. Business Change Management	0,00%	0,00%

Table 63. Croatia - Competences from training offerings according to percentual frequency

Co-funded by the European Union

	ECSF Role	%match	St.Dev.	#No1	#No2	#No3
1	Cybersecurity Risk Manager	4,95%	10,63%	16	1	0
2	Cyber Threat Intelligence Specialist	3,08%	7,22%	10	4	0
3	Cybersecurity Researcher	2,64%	6,77%	2	10	0
4	Cyber Incident Responder	2,42%	6,52%	10	1	0
5	Penetration Tester	1,32%	4,96%	5	1	0
6	Cybersecurity Implementer	0,88%	4,10%	1	3	0
7	Cybersecurity Educator	0,37%	3,48%	1	0	0
8	Cyber, Legal, Policy & Compliance Officer	0,28%	2,61%	0	1	0
9	Chief Information Security Officer (CISO)	0,00%	0,00%	0	0	0
10	Cybersecurity Architect	0,00%	0,00%	0	0	0
11	Cybersecurity Auditor	0,00%	0,00%	0	0	0
12	Digital Forensics Investigator	0,00%	0,00%	0	0	0

Table 64. Croatia - ECSF Roles, average, standard deviation and top 3 education offerings

Co-funded by the European Union

Vacancy Tables – Overall

Competences	Total	SME	Public Professionals
A.1. IS and Business Strategy Alignment	5,61%	1,49%	2,64%
A.2. Service Level Management	0,50%	0,50%	0,17%
A.3. Business Plan Development	0,99%	0,99%	0,66%
A.4. Product/Service Planning	0,66%	0,50%	0,99%
A.5. Architecture Design	10,07%	4,62%	2,31%
A.6. Application/Product Design	3,14%	1,49%	1,65%
A.7. Technology Trend Monitoring	10,56%	2,97%	6,27%
A.8. Sustainability Management	0,83%	0,00%	0,00%
A.9. Innovating	0,50%	0,50%	0,66%
A.10. User Experience	1,65%	0,99%	0,33%
B.1. Application/Product Development	5,78%	4,62%	3,30%
B.2. Component Integration	6,27%	2,15%	0,66%
B.3. Testing	12,21%	4,13%	1,98%
B.4. Solution Deployment	8,75%	1,49%	2,81%
B.5. Documentation Production	14,69%	5,45%	4,46%
B.6. ICT Systems Engineering	7,92%	4,13%	1,16%
C.1. User Support	5,61%	3,47%	1,49%
C.2. Change Support	4,46%	1,32%	0,50%
C.3. Service Delivery	3,30%	1,49%	1,65%
C.4. Problem Management	16,17%	6,77%	4,95%
C.5. Systems Management	11,55%	5,78%	2,64%
D.1. Information Security Strategy Development	11,88%	3,96%	4,62%
D.2. Quality Strategy Development	2,15%	0,50%	0,66%
D.3. Education and Training Provision	7,92%	2,64%	4,13%
D.4. Purchasing	1,49%	0,66%	0,66%
D.5. Sales Development	0,83%	0,99%	0,99%
D.6. Digital Marketing	0,17%	0,00%	0,00%
D.7. Science and Analysis	9,41%	4,13%	7,26%
D.8. Contract Management	1,16%	0,50%	0,50%
D.9. Personnel Development	1,98%	1,49%	2,31%
D.10. Information and Knowledge Management	3,47%	1,98%	2,31%
D.11. Needs Identification	4,13%	2,81%	1,98%
D.12. Security Consulting	11,06%	9,74%	9,74%
E.1. Forecast Development	1,16%	0,00%	0,00%
E.2. Project and Portfolio Management	3,63%	1,49%	3,47%
E.3. Risk Management	17,82%	3,47%	1,65%
E.4. Relationship Management	3,96%	4,29%	6,44%
E.5. Process Improvement	3,47%	1,16%	1,16%
E.6. Quality Management and Compliance	9,08%	2,97%	2,48%
E.7. Business Change Management	2,48%	0,66%	0,50%
E.8. Information Security Management	21,45%	3,80%	3,14%
E.9. Information Systems Governance	6,60%	0,83%	1,32%

Table 65. The Netherlands, Cyprus, Croatia – Average percentages of total vacancies, SMEs and Public Professionals

Co-funded by the European Union

ECSF Role		NL	CY	CR	AVG%
1	Cyber, Legal, Policy & Compliance Officer	4,14%	4.27%	19,27%	7,80%
2	Cybersecurity Educator	4,76%	3.25%	14,23%	6,33%
3	Cybersecurity Researcher	3,93%	1.95%	10,24%	4,72%
4	Digital Forensics Investigator	2,69%	13.41%	10,67%	4,45%
5	Cyber Threat Intelligence Specialist	6,46%	0.98%	6,10%	4,19%
6	Cybersecurity Implementer	4,97%	4.39%	6,83%	3,93%
7	Cybersecurity Auditor	3,39%	0.00%	6,59%	3,33%
8	Chief Information Security Officer (CISO)	3,39%	2.93%	6,59%	3,33%
9	Cyber Incident Responder	3,39%	9.76%	6,34%	3,24%
10	Cybersecurity Architect	4,31%	1.46%	5,12%	3,14%
11	Cybersecurity Risk Manager	2,43%	1.83%	6,10%	2,84%
12	Penetration Tester	1,78%	0.49%	6,59%	2,79%

Table 66. The Netherlands, Cyprus, Croatia – Average ECSF role match percentage for vacancies

Co-funded by the European Union

Education Tables – Overall

Competences	Total	Education	Courses	Trainings
A.1. IS and Business Strategy Alignment	11,24%	6,83%	2,81%	1,61%
A.2. Service Level Management	1,20%	1,20%	0,00%	0,00%
A.3. Business Plan Development	4,82%	4,02%	0,00%	0,80%
A.4. Product/Service Planning	6,83%	6,43%	0,00%	0,40%
A.5. Architecture Design	30,12%	21,29%	4,42%	4,42%
A.6. Application/Product Design	22,49%	21,29%	0,00%	1,20%
A.7. Technology Trend Monitoring	19,68%	11,24%	4,82%	3,61%
A.8. Sustainability Management	4,02%	4,02%	0,00%	0,00%
A.9. Innovating	3,21%	2,41%	0,00%	0,80%
A.10. User Experience	12,05%	11,24%	0,00%	0,80%
B.1. Application/Product Development	32,93%	29,72%	1,20%	2,01%
B.2. Component Integration	24,10%	19,68%	2,01%	2,41%
B.3. Testing	33,73%	14,86%	11,24%	7,63%
B.4. Solution Deployment	23,29%	13,65%	6,83%	2,81%
B.5. Documentation Production	24,50%	16,06%	5,62%	2,81%
B.6. ICT Systems Engineering	30,92%	20,08%	4,82%	6,02%
C.1. User Support	9,24%	8,03%	0,00%	1,20%
C.2. Change Support	6,43%	4,02%	1,61%	0,80%
C.3. Service Delivery	6,43%	4,42%	1,20%	0,80%
C.4. Problem Management	33,73%	14,86%	11,65%	7,23%
C.5. Systems Management	41,37%	22,89%	12,05%	6,43%
D.1. Information Security Strategy Development	14,86%	3,61%	6,02%	5,22%
D.2. Quality Strategy Development	3,61%	3,21%	0,40%	0,00%
D.3. Education and Training Provision	8,03%	4,42%	2,01%	1,61%
D.4. Purchasing	2,81%	2,41%	0,40%	0,00%
D.5. Sales Development	0,80%	0,80%	0,00%	0,00%
D.6. Digital Marketing	0,80%	0,80%	0,00%	0,00%
D.7. Science and Analysis	39,36%	25,70%	10,04%	3,61%
D.8. Contract Management	1,20%	0,00%	0,40%	0,80%
D.9. Personnel Development	8,03%	5,22%	0,40%	2,41%
D.10. Information and Knowledge Management	9,64%	6,02%	1,20%	2,41%
D.11. Needs Identification	15,66%	13,25%	1,61%	0,80%
D.12. Security Consulting	18,07%	7,63%	7,63%	2,81%
E.1. Forecast Development	5,62%	3,61%	2,01%	0,00%
E.2. Project and Portfolio Management	20,88%	16,06%	2,81%	2,01%
E.3. Risk Management	41,77%	12,85%	14,86%	14,06%
E.4. Relationship Management	12,85%	8,84%	2,41%	1,61%
E.5. Process Improvement	15,66%	13,25%	2,41%	0,00%
E.6. Quality Management and Compliance	28,51%	10,04%	10,84%	7,63%
E.7. Business Change Management	9,24%	6,02%	2,41%	0,80%
E.8. Information Security Management	60,24%	22,89%	19,28%	18,07%
E.9. Information Systems Governance	21,29%	7,63%	6,43%	7,23%

Table 67. The Netherlands, Cyprus, Croatia – Average percentages of (total) trainings, courses and education offerings

Co-funded by the European Union

ECSF Role		NL	CY	CR	AVG%
1	Cyber Threat Intelligence Specialist	4,50%	3,16%	3,08%	3,58%
2	Cybersecurity Risk Manager	3,57%	0,00%	4,95%	2,84%
3	Cybersecurity Researcher	1,09%	0,00%	2,64%	1,24%
4	Cyber Incident Responder	0,82%	0,00%	2,42%	1,08%
5	Penetration Tester	0,82%	0,00%	1,32%	0,71%
6	Cybersecurity Educator	0,68%	0,00%	0,37%	0,35%
7	Cybersecurity Implementer	0,00%	0,00%	0,88%	0,29%
8	Cyber, Legal, Policy & Compliance Officer	0,34%	0,00%	0,28%	0,21%
9	Digital Forensics Investigator	0,51%	0,00%	0,00%	0,17%
10	Chief Information Security Officer (CISO)	0,00%	0,00%	0,00%	0,00%
11	Cybersecurity Architect	0,00%	0,00%	0,00%	0,00%
12	Cybersecurity Auditor	0,00%	0,00%	0,00%	0,00%

Table 68. The Netherlands, Cyprus, Croatia – Average ECSF role match percentage for trainings, courses and education offerings

Co-funded by the European Union

Annex 7 Results focus groups

Pilot focus group

We asked the participants of the focus group to reflect on four trends identified in the trend analysis:

#1 Increase in complex and sophisticated threats	• Cyberattacks are becoming increasingly technical, targeted, and automated, with the rise of APTs, nation-state actors, and AI-generated attacks such as deepfakes and sophisticated phishing.
#2 Shift to cloud and hybrid infrastructure	The rapid adoption of cloud platforms such as Azure, AWS, and Google Cloud requires new expertise in cloud-native security, zero trust architectures, and the security of hybrid IT environments.
#3 New and stricter laws and regulations	• New frameworks such as NIS2, DORA and the revision of the GDPR are forcing organisations to structurally manage risk and make targeted investments in security awareness and process-based security roles
#4 Automation and AI in security operations	• AI is increasingly being used for threat detection and anomaly analysis in security platforms, but it also requires new skills around ethics, bias and dealing with AI-driven threats

According to participants, the four cybersecurity trends are intertwined. For example: an increase in complex threats (trend #1), is caused by a shift to cloud and hybrid infrastructures (trend #2), and by criminals using automation and AI to execute cyberattacks (trend #4)

Cybersecurity trend 1: Increase in complex and sophisticated threats
Reflection of participants:

- Threats are more often aimed at stealing privacy-sensitive data to pressure companies and individuals.
- At the government level, military hybrid threats are a real risk.
- Failure of critical infrastructure could result in severe disruption.
- Scenario planning is needed: how can the government respond to incidents effectively?

Cybersecurity trend 2: Shift to cloud and hybrid infrastructure
Reflection of participants:

- We should not only focus on Information Technology (IT) but also on Operational Technology (OT). This requires a different specialism.
- We should be aware of the dependencies on Big Tech (for example, Microsoft), and the implications of these dependencies for cybersecurity.
- Try to pursue independence by making conscious choices, consider European alternatives: https://european-alternatives.eu/.

Cybersecurity trend 3: New and stricter laws and regulations
Reflection of participants:

- NIS-2 legislation does not apply to small SMEs (< 50 employees), unless they are suppliers of an organisation that does fall under the NIS-2.
- The impact of NIS-2 on municipalities is great; it is a major challenge to meet these requirements.
- In addition to risk management within companies, attention should also be paid to risk management at societal level.

Cybersecurity trend 4: Automation and AI in security operations
Reflection of participants:

Co-funded by the European Union

- AI not only amplifies cyber threats but also digital crime (for example: deepfake fraud). Awareness and training around digital crime and fraud within companies is needed.
- The AI quadrant shows the impact of AI on cybersecurity challenges and opportunities. [9]

General reflections:
- The level of cybersecurity skills within companies varies and depends on the type of company.
- Small entrepreneurs often lack the basic skills to protect systems, prepare for incidents and train employees on cybersecurity.
- Within (small) municipalities, there is a shortage of personnel to properly organise cybersecurity and meet the NIS-2 requirements.
- Agencies such as the Information Security Service offer advice and support (for example: checklists, emergency plans, incident response support).
- However, it is not always clear whether the realisation of cybersecurity measures is a governmental or technical responsibility.

Three implications for education have been identified:
- There should be a stronger focus on the **development of soft skills** among IT professionals and employers, to stimulate mutual understanding and healthy behaviour in organisations.
- More attention should be paid to **ethical issues**, for example by practicing ethical hacking in controlled settings ("capture the flag").
- **Interdisciplinarity in education** is important. Cybersecurity is not only the responsibility of IT professionals, but of all layers in the organisation.

Conclusions:
- There are **three major challenges** around cybersecurity in the Netherlands
  - A lack of basic cyber security skills,
  - Staff shortages on a technical and managerial level (e.g. CISO)
  - Role ambiguity around the implementation of cybersecurity.
- To **become cyber resilient**, organisations must work on:
  - Prevention (emergency plans, risk management)
  - Protection (securing systems, devices and applications)
  - Promotion (promoting cybersafe behaviour)
  - Preparation (being equipped to respond to incidents)
- Organisations need proper support from **experts and authorities** in cybersecurity.
- Greater responsibilities must be placed on **suppliers and service providers** to deliver secure systems.
- In **education**, more attention should be paid to soft skills, leadership/management skills, ethics and interdisciplinary working.

Co-funded by the European Union

Focus group 1a: Representatives public sector

Selection criteria participants:

- Representatives of public organisations (ministries, education)
- Good understanding of cybersecurity labour market needs and education
- Familiar with national agendas
- Can identify and assess the necessary competences, skills/knowledge, and tasks required for the sector
- Familiar with reports and analyses and has access to these data sources/trend reports
- Knows the ECSF roles and e-CF ICT competences and can identify these for the sector
- Can effectively consult with other experts about future developments that impact current competences
- Aware of future changes in technical developments, security changes, risks, etc., and what these demands from the sector.

Part 1: Specifying trends in cybersecurity

Cybersecurity Trend 1. AI-enhanced cyber threats and digital deception

- Participants confirmed the rise of AI-driven threats, especially deepfakes and synthetic voices used in phishing and social engineering campaigns.
  - A participant noted: "*These trends are not hypothetical anymore. We've already seen fake voice messages used to impersonate senior officials*."
- A participant from Cyprus emphasised that spear phishing is a daily threat to government agencies, with no current AI-based defence tools in place. Instead, they rely heavily on awareness efforts.
- Several participants noted the need for proactive, AI-enabled defence strategies, beyond traditional reactive tools.

Cybersecurity Trend 2: Digital dependencies and governance under pressure

- Participants confirmed increasing reliance on non-EU cloud providers (e.g., Azure, AWS), raising concerns about digital sovereignty, long-term vendor lock-in, and compliance with regulations such as NIS2.
  - A participant put it: "*We've built critical services on clouds we don't control—this puts our sovereignty at risk.*"
- Greek participants highlighted the potential of the national G-Cloud initiative, aimed at reducing foreign dependencies. However, challenges remain in terms of capacity, scalability, and availability of skilled professionals.
  - A participant described: "*The G-Cloud could be a game changer, but we're still facing issues with scale, staffing, and long-term investment.*"
- Participants emphasised that increased outsourcing and use of commercial cloud services create complex supply chain dependencies, which heighten the risk of cyberattacks and complicate regulatory compliance.

Co-funded by the European Union

Cybersecurity Trend 3. Governance resilience and recovery capabilities

- Participants strongly agreed with the focus on cyber resilience and recovery, especially because ransomware attacks can shut down public services and damage data.
- Greek participants shared recent high-impact examples, including ransomware attacks on universities and critical services like the Greek Cadastre, as well as DDoS and APT threats targeting ministries and financial institutions. These incidents highlighted the urgent need for operational continuity planning and rapid response mechanisms.
- Participants emphasised that resilience must go hand-in-hand with prevention and cross-sector collaboration. Recovery capabilities alone are not sufficient—investment in prevention, shared responsibilities, and inter-organisational coordination is essential to protect public functions.
    - A participant put it: "We urgently need more cooperation—both in preventing incidents and in how we respond to them."

Are there any key developments you feel are missing from the trends as described?

- Fragmented IT makes it harder to act quickly and clearly.
  IT systems are now spread across many locations, devices, and external partners. This creates new risks. Many organisations no longer have a clear overview, and during a cyber incident, it's often unclear who should do what—especially in local governments, this slows down response.
    - A participant described: "IT is no longer confined within secure walls; it's flying, driving, and walking around — and often outside our direct control."
- Key sectors and suppliers don't get enough attention.
  Important sectors like energy, transport, and surveillance face growing cyber risks but aren't well protected. At the same time, many companies depend on outside suppliers without properly checking if their cybersecurity is in order. That's a weak link.
- Cybersecurity is not just for IT experts.
  Digital threats are becoming smarter and often trick people, not just systems. That's why it's important that everyone—not just IT staff, but also employees, managers, and citizens—understands how to stay safe. Cybersecurity is a shared responsibility.
    - A participant stressed: "Deepfake scams and AI-generated voice attacks show we need to focus much more on digital literacy for the general public."

How does the shortage of cybersecurity professionals affect your countries or organisation's capacity to respond effectively to these trends?

- Staff shortages affect the entire cybersecurity cycle.
  Public organisations often lack sufficient personnel to manage prevention, detection, response, and recovery effectively. In many cases, individuals must handle multiple roles simultaneously, and limited professional certification further reduces operational capacity.
    - A participant described: "One person is often responsible for everything—from detection to recovery. That's simply not sustainable."

Co-funded by the European Union

- There is a structural gap in cybersecurity talent development.
  The absence of undergraduate programmes, combined with a mismatch between academic training and real-world job needs, limits the inflow of qualified professionals—especially in the public sector.
- Governance and compliance are weakened by lack of senior expertise.
  Key roles such as CISOs are difficult to fill, which undermines strategic coordination, regulatory implementation (e.g., NIS2), and the ability to respond to complex threats.
  - A participant stressed: "The shortage of qualified CISOs limits our ability to coordinate strategy and comply with NIS2."

Considering the growing shortage of cybersecurity professionals, which of the three trends do you see as the most challenging to address — and why?

According to participants:

- The biggest challenge lies in translating complex cybersecurity issues to board-level decision-making.
  There is a persistent communication gap between technical experts and executive leadership, making it difficult to secure strategic support and resources. This affects all trends but is especially critical for AI-related risks and long-term resilience.
  - A participant stressed: "When I talk about AI with our board, they say: 'Oh yes, my nephew showed me ChatGPT.' That's the level we're dealing with."
- The skill shortage goes beyond technical roles – cross-domain capabilities are lacking.
  Cybersecurity experts often aren't trained to deal with new technologies like AI, IoT, or drones. At the same time, other people in the organisation may not know enough to properly check or manage the security they've outsourced.
  - A participant described: "Security is still treated as something you do after the functional design phase. That mindset has to change."
- The current mindset and frameworks are outdated for future threats.
  Existing cybersecurity approaches focus on classic IT environments, while modern threats require new ways of thinking, integrated frameworks, and collaboration across sectors. This is especially urgent given the increasing reliance on external contractors and the lack of internal expertise.
  - A participant stressed: "Our current methods are not equipped for the IT of the future. We're using yesterday's security for tomorrow's technology."
- Low public sector salaries and dependence on contractors increase vulnerability.
  Many public organisations struggle to attract and retain qualified professionals, leading to over-reliance on external providers without sufficient in-house knowledge to manage or assess them.
  - A participant described: "In Cyprus, with our current government wages, we simply can't hire cybersecurity staff. We rely almost entirely on private contractors".

Co-funded by the European Union

Part 2: specifying implications cybersecurity trends for competences and skills

In your view, which (technical and content-specific) cybersecurity competences are currently needed to effectively address the aforementioned cybersecurity trends?

Competence Area	Description	Examples of Tasks or Activities
1. AI-Aware Cyber Threat Response	Cybersecurity professionals need new skills to spot, understand, and respond to threats that are powered by AI. They should be able to use AI tools and data to detect suspicious activity—while also knowing the risks of relying too much on these technologies.	• Using AI or machine learning to detect unusual behaviour or patterns • Critically reviewing AI results for bias, false alarms, or limitations • Identifying and stopping AI-powered attacks like deepfakes or automated phishing emails
2. Cloud & Supply Chain Security	Cybersecurity professionals need the skills to keep cloud environments secure and manage the risks that come with using third-party providers. This includes checking if vendors meet security standards and following new regulations like NIS2 and DORA.	• Securing hybrid cloud setups and spotting mistakes in configuration • Assessing the cybersecurity of vendors and keeping track of their compliance • Explaining cloud-related security risks in terms that business leaders understand
3. OT and IoT Cybersecurity	Cybersecurity professionals need skills to secure operational technology (OT), Internet of Things (IoT), and other systems that connect the digital and physical world. These systems often fall outside traditional IT security and require a different approach.	• Protecting devices like bodycams, drones, and industrial sensors • Applying security best practices to physical systems connected to the internet • Designing OT systems with security built into the architecture from the start
4. Cyber Incident Response and Recovery	Cybersecurity professionals need to be able to detect and respond to cyber incidents quickly, and help systems recover with as little downtime as possible. This includes planning ahead to keep services running and protect critical functions in society during and after an attack.	• Managing backups and systems that help recover after a disruption • Responding to incidents, finding the root cause, and fixing the problem • Planning recovery and continuity with other teams or organisations
5. Strategic Cybersecurity Governance	Cybersecurity professionals need to connect cybersecurity with the organisation's overall goals. This means helping leadership understand cyber risks, making sure security is part of decision-making, and building a strong security culture across departments.	• Explaining technical risks in clear, business-focused language • Linking cybersecurity to legal, financial, and operational priorities • Leading organisation-wide efforts to improve security awareness and responsibility

Co-funded by the European Union

6. DevSecOps Practices and Secure Development	Cybersecurity professionals need the skills to build security into software from the very beginning—especially in fast-paced environments like agile and DevOps. Security should be part of design, development, and testing, not just something added later.	• Applying secure-by-design principles within agile development teams • Performing threat modelling and designing secure APIs • Integrating security checks and testing into CI/CD pipelines

In your view, which soft skills are currently needed to effectively the aforementioned cybersecurity trends?

Competence Area	***Description***	***Practical application***	***Quote***
1. Communication & Risk Translation	The ability to clearly explain cybersecurity issues to non-technical stakeholders, including board members, users, and external partners.	• Write clear incident reports and risk analyses. • Present security issues at executive level. • Translate technical problems into business language.	One participant noted the challenge of being taken seriously by leadership: 'You have to grow a beard before they listen.'
2. Leadership, Decision-Making & Organisational Awareness	The capacity to take responsibility in critical situations and navigate decision-making processes within complex public sector environments.	• Lead during crisis response and recovery. • Make timely decisions under uncertainty. • Align cybersecurity actions with organisational risk appetite and culture.	A participant shared: 'No one takes decisions about awareness or incident response. We need people who are able to decide.'
3. Ethical Awareness & Societal Responsibility	The ability to recognise and act upon the ethical dimensions of cybersecurity, especially with emerging technologies.	• Balance security measures with transparency and proportionality. • Evaluate ethical risks of AI and surveillance systems. • Promote responsible data and technology use.	
4. Analytical Thinking & Learning Agility	The skill to interpret complex threats and stay current with fast-evolving technologies.	• Analyse threat patterns and risk signals. • Adapt to new technologies and methodologies. • Maintain a learning mindset in a dynamic field.	
5. Collaboration & Boundary-Spanning	The ability to work across departmental, organisational and disciplinary boundaries, including with external vendors.	• Manage vendor relationships with security expertise. • Collaborate across IT, legal, procurement, and leadership. • Build trust and shared responsibility across stakeholders.	

Co-funded by the European Union

How do you experience competence gaps in practice?

- Strategic and governance-related roles are most affected.
    - There are gaps in roles where cybersecurity must be integrated into governance and long-term planning.
    - Professionals who can align IT investments with public service missions or organisational priorities are often hard to find.
    - Many candidates for strategic roles such as CISO lack the combined technical expertise and organisational insight needed to work effectively across leadership and stakeholder groups.
- Cybersecurity is still viewed primarily as a technical issue.
    - Cybersecurity is still too often treated as a purely technical issue instead of a governance concern.
    - There is limited capacity to connect cybersecurity needs with broader policy goals, legal frameworks, and mission-driven operations.

What kind of practical challenges do these gaps create for you or your work?

- Delayed or misinformed decision-making. Decisions around cybersecurity strategy, investment or compliance are often made without proper understanding of scope or risk. In some cases, external consultants drive key decisions without internal teams having the skills to critically assess them.
- Dependency on external consultants without sufficient oversight. Organisations rely on consultancy for NIS2, but often lack the in-house knowledge to manage, guide or evaluate their input. This undermines sustainable capability building.
- Compliance and continuity risks. When organisations lack knowledge in strategic security planning or risk management, they often miss compliance deadlines, struggle with implementation, and face higher chances of disruption.
- Communication gaps between technical and non-technical teams. Participants reported weak coordination between IT teams and senior management. This delays investment, hinders urgency, and obstructs alignment between cybersecurity needs and organisational priorities.

Part 3: conclusions

1. A shortage of qualified professionals leaves organisations exposed.

- Many public organisations face an ongoing shortage of cybersecurity talent.
- As a result, key roles are often concentrated in the hands of one or two individuals who must juggle responsibilities.
- Recruiting staff with both deep technical expertise and an understanding of legal, strategic, and policy issues proves to be difficult.

Co-funded by the European Union

- This leads to vacancies in pivotal roles like Chief Information Security Officer (CISO), or positions being filled without the necessary qualifications.
- Consequently, organisations become overly reliant on external consultants, miss critical compliance deadlines (such as those under NIS2), and respond too slowly or inadequately to attacks.

2. Without soft skills, cybersecurity remains stuck in a technical silo.

- Effective cybersecurity requires more than technical acumen, it depends on strong interpersonal and decision-making skills.
- Participants noted a recurring disconnect between IT professionals and leadership, which often results in delayed or ignored security recommendations.
- What is lacking are professionals who can communicate complex risks clearly, make rapid decisions under pressure, and navigate ethical dilemmas related to emerging technologies such as AI.
- Soft skills like cross-functional collaboration, ethical judgment, and clear communication are not optional add-ons.
- They are essential for converting technical insights into actionable strategies, gaining buy-in across the organisation, and ensuring business continuity in times of crisis.

Focus group 1b: Representatives private sector

Selection criteria participants:

- Representatives of private organisations (employers' associations, cybersecurity hubs, private training representatives; at least 1 representative from SMEs (SME = => 250 employees))
- Good understanding of cybersecurity labour market needs and education
- Familiar with national agendas
- Can identify and assess the necessary competences, skills/knowledge, and tasks required for the sector
- Familiar with reports and analyses and has access to these data sources/trend reports
- Knows the ECSF roles and e-CF ICT competences and can identify these for the sector
- Can effectively consult with other experts about future developments that impact current competences
- Aware of future changes in technical developments, security changes, risks, etc., and what these demands from the sector.

Part 1: Specifying trends in cybersecurity

Cybersecurity Trend 1. AI-enhanced cyber threats and digital deception

- AI was specifically highlighted as a rapidly growing factor in both offensive and defensive cybersecurity activities.

Co-funded by the European Union

- A participant observed: “AI is becoming one of the hottest topics in cybersecurity—from both the defensive and offensive side. It’s becoming mandatory to adapt”.
- Participants said that AI is already affecting incident response and penetration testing by automatically creating scripts and helping to develop more advanced malware.

Cybersecurity Trend 2. Digital dependencies and compliance challenges

- Participants confirmed that the shift to multi-cloud environments and growing reliance on third-party services complicate cybersecurity governance. Managing a diverse ecosystem becomes especially challenging when onboarding procedures are unclear or inconsistent.
    - A participant described: “The move to cloud architectures, often involving a mix of providers and partners, makes cybersecurity governance a challenge—especially when onboarding new services isn’t well defined.”
- SMEs, particularly non-ICT companies, face disproportionate compliance burdens under regulations such as NIS2 and DORA. Limited staff capacity, high implementation costs, and fragmented legal requirements make it difficult to meet security standards effectively.
    - A participant noted: “The cost to comply is huge for a smaller SME.” and one participant added: “Meeting all the different regulations is a real challenge, especially for non-ICT companies.”
- Participants also said that clients are paying more attention to data privacy and cloud use. Companies now need to explain why they choose certain providers and show they handle digital tools responsibly.

Cybersecurity Trend 3. Operational resilience and incident response readiness

- Participants said that rules like DORA are pushing private companies to focus more on being operationally resilient. They are expected to get better at preparing for and responding to incidents, using both technical and organisational solutions.
- Several participants observed increased demand from clients for support in building resilience. This includes practical help with backup strategies, continuity planning, and the implementation of recovery protocols.
- At the same time, smaller businesses often lack the resources to invest in comprehensive testing or long-term planning. Although basic protections may be in place, many organisations have yet to validate how well they can respond when a serious incident occurs.
    - A participant shared: “We’ve implemented a lot of security features and backups for our customers, but we don’t really know how strong we are—we haven’t had a breach yet, and we don’t have the resources for large-scale testing.”

2. How does the shortage of cybersecurity professionals affect your company’s or sector’s ability to effectively respond to these trends?

Co-funded by the European Union

- Staffing shortages affect the sector unevenly but significantly.
  SMEs in particular struggle to attract qualified cybersecurity talent for critical roles, often leaving tasks to underqualified staff or relying on outdated procedures to cope.
    - A participant noted: “What we see happening instead is sticking to outdated procedures or relying on other departments with no cybersecurity skills.”
- The lack of implementation capacity limits both service delivery and innovation.
  Participants said that having too few people makes it harder to expand cybersecurity work, respond quickly to incidents, and deliver high-quality services to clients.
- Companies are forced to re-skill internal IT staff or stretch existing teams.
  Because there is little external support available, companies often rely on quickly training their own staff or asking teams to take on extra tasks. This can reduce the quality of their work and make it harder to keep up with new cybersecurity threats.
    - A participant noted: “We’re doing as much as we can, but without security professionals, we just hope we can find a solution.” and one participant added: “If demand keeps rising, clients may have to wait longer for reports and incident support.”

3. Considering the growing shortage of cybersecurity professionals, which of the three trends do you see as the most challenging to address — and why?

- Compliance obligations outpace internal capacity.
  Organisations, especially SMEs, are overwhelmed by the speed and complexity of cybersecurity regulation such as NIS2 and DORA. The lack of qualified staff makes it difficult to meet these requirements without panic-driven, short-term fixes. This challenge affects both vendors and service providers who are expected to support clients while managing their own compliance.
    - A participant noted: “NIS2 and DORA have created a lot of panic among IT guys. We’re all fixing firewalls, enabling 2FA, cutting user permissions—just trying to keep up.” and one participant added: “For us as a vendor, complying with all these regulations takes enormous resources—and our clients expect us to help them too.”
- AI requires deep, targeted expertise that many companies lack.
  AI is seen as important for both innovation and defence against threats, but many organisations can’t find enough people who know how to use it safely and effectively. The lack of cybersecurity staff with AI skills makes it harder to adopt these tools properly and increases the risk of mistakes or misuse.
    - A participant noted: “The main challenge is finding the right AI expertise to actually improve our capabilities, not just follow hype.”

3. Considering the growing shortage of cybersecurity professionals, which of the three trends do you see as the most challenging to address — and why?

According to participants:

- Resilience demands more than technical skills – it requires strategic oversight.
  Participants highlighted that true resilience depends on people who understand the broader impact of incidents and can plan for continuity. Due to staff shortages, these roles are often

Co-funded by the European Union

filled by overburdened IT generalists, leaving organisations unprepared for high-impact disruptions.

  - A participant noted: "We try to prepare clients, but many still lack the ability to see how downtime will really affect their operations."

- The greatest gap lies in experienced professionals who see the full picture.
  There is a shortage of senior cybersecurity staff who can connect technology, regulation, and business priorities. Without this leadership capacity, organisations struggle to develop coherent strategies or respond to complex, cross-cutting risks.

  - A participant mentioned: "We can find penetration testers, sure—but people who understand the wider picture, who can align technology, compliance, and strategy? Those are rare." and one participant added: "You don't want to hand everything over to external firms, but you also can't build it all in-house without the right people. That's our dilemma."

In your view, which (technical and content-specific) cybersecurity competences are currently needed to effectively address the aforementioned cybersecurity trends?

Competence Area	**Description**	**Examples of Tasks or Activities**
1. Operational Cloud Security Management	*Cybersecurity professionals need the skills to secure cloud environments by setting the right access controls, detecting threats, and making sure systems follow security standards and laws. This also includes managing risks across different cloud providers.*	• *Setting and managing access rights for cloud users and systems* • *Identifying and handling security risks in multi-cloud environments* • *Monitoring cloud setups for mistakes, misconfigurations, or policy violations*
2. OT Risk Management and Compliance	*Cybersecurity professionals need the skills to protect industrial control systems and operational technology (OT), especially in vital sectors like energy, transport, and water. These systems often run separately from regular IT and need their own security approach—one that includes risk analysis and compliance with rules like NIS2.*	• *Separating (segmenting) OT networks from other systems to limit damage from attacks* • *Identifying and managing risks specific to industrial control systems* • *Applying cybersecurity rules and requirements such as NIS2 to OT environments*
3. Incident Detection and Investigation	*Cybersecurity professionals need the ability to detect, investigate, and respond to cyber incidents. This includes analysing what happened after an attack, collecting digital evidence, and using that information to prevent future incidents.*	• *Reviewing what went wrong after a cyber incident (post-incident analysis)* • *Collecting and interpreting system logs and security alerts* • *Performing forensic analysis to trace the source and method of an attack*
4. Secure Software Architecture and Development	*Cybersecurity professionals need to know how to build systems and applications that are secure from the start. This means thinking about security early in the design process, choosing safe components, and making sure that every step of development includes the right protections.*	• *Identifying potential threats before development begins (threat modelling)* • *Choosing secure building blocks, such as frameworks and APIs* • *Including security checks throughout the software development lifecycle (SDLC)*

Co-funded by the European Union

5. Cyber Risk Management and Strategic Alignment	*Cybersecurity professionals need to identify and assess cybersecurity risks, decide which ones matter most, and make sure their security strategy supports business goals and follows legal requirements. They must also explain risks clearly to leadership.*	• *Performing risk assessments using qualitative or quantitative methods* • *Communicating key risks in a way that business leaders understand* • *Aligning security controls with laws and standards like NIS2*

In your view, which soft skills are currently needed to effectively the aforementioned cybersecurity trends?

Competence Area	Description	Practical application	*Quote*
Communication	The ability to clearly convey complex cybersecurity issues to various audiences, including non-technical stakeholders and executive leadership.	Used to report security risks to board members, justify investments, and ensure compliance communication.	*One participant shared: 'When I talk about AI and security, the board says: My nephew showed me ChatGPT.'*
Critical and Analytical Thinking	The ability to analyse complex threats, challenge assumptions, and develop appropriate responses based on sound reasoning.	Applied in incident assessment, threat prioritisation, and evaluating new technologies or regulatory requirements.	*One participant noted: 'We need people who don't just follow protocols but can find new ways to solve unexpected problems.'*
Adaptability & Learning Agility	The capacity to adjust to new technologies and threats quickly and to proactively learn emerging tools and practices.	Needed to adopt new defensive tools, adjust to AI-driven threats, and respond to rapidly changing threat landscapes.	*Participants emphasised the need to 'live with the field' and continuously self-educate beyond the formal workday.*
Ethical Awareness & Responsibility	The awareness of ethical implications in cybersecurity actions, and the ability to act with integrity and accountability.	Essential when setting data governance policies or responding to ethically sensitive incidents, such as AI misuse.	*One participant stated: 'You need to understand the fear you instil with certain messages, and act proportionally.'*
Collaboration	The ability to work across functions and disciplines to coordinate cybersecurity activities effectively.	Enables cross-domain response teams to function during crises or to design integrated cybersecurity policies.	*A participant shared: 'We solve problems faster when criminologists and IT professionals' team up.'*

How do you experience these competence gaps in practice?

- Transition from theory to practice remains difficult
  Participants noted that applying theoretical knowledge in real-world settings is a persistent challenge, especially for junior professionals. Skills in areas such as data science or

Co-funded by the European Union

application development do not always translate into effective practice, slowing down professional growth.

- Progression from junior to senior roles takes more time and support
  It takes increasingly longer to train junior staff to a senior level across cybersecurity roles. This puts pressure on teams, particularly in specialised domains such as system design or incident response.
- Lack of certification and practical focus in foundational training
  While general knowledge may be available through public education or training, entry-level professionals often lack internationally recognised certifications. In more advanced areas, such as consulting, the lack of experience-based learning further contributes to skill gaps.

What kind of practical challenges do these gaps create for you or your work?

- Junior professionals often lack essential skills, leading to delays and higher onboarding costs
  Employers report that new hires frequently lack the expected baseline knowledge. This creates extra work for senior staff and slows down both project execution and problem resolution.
- Organisations hesitate to invest in inexperienced staff, further limiting talent pipelines
  Because of the intensive support required, some organisations bypass junior talent altogether. This contributes to a long-term shortage of cybersecurity professionals and reinforces hiring difficulties.
- Upskilling internal staff is the most common response but stretches capacity
  Due to limited availability of qualified candidates, most organisations rely on training existing personnel. While practical, this strategy slows down operations and creates pressure on already scarce resources.

Part 3: conclusions

- The three proposed cybersecurity trends are widely recognised in the private sector.
- In particular, Trend 2 (compliance and digital dependencies) is seen as the most difficult to address.
- The combination of complex regulations (such as NIS2 and DORA) and limited internal capacity causes organisations to fall behind.
- This is especially true for small and medium-sized enterprises (SMEs), which struggle to consistently manage multi-cloud environments and to oversee third-party vendors responsibly.
- The trend exposes the fact that many organisations still lack adequate control over their digital supply chains—primarily due to weak governance processes (‘E.9. Information Systems Governance’), insufficient risk management (‘E.3. Risk Management’), and gaps in cloud security capabilities (‘B.6. ICT Systems Engineering’ and ‘A.5. Architecture Design’).
- These technical competences are essential for managing third-party risks, ensuring regulatory compliance, and maintaining secure cloud environments.

Co-funded by the European Union

- Staffing shortages make it difficult for many organisations to respond adequately to emerging threats.
- AI applications (Trend 1) require specialised technical competences, such as data analysis, threat detection, and the responsible use of AI tools—skills that are in short supply.
- At the same time, Trend 3 (operational resilience) demands both technical incident response skills and strategic insight for crisis preparedness.
- The impact is greatest in small SMEs, where a single IT professional often has to juggle multiple roles—from cloud management to incident response.
- This leads to delays, vulnerabilities, and a heavy reliance on external parties.
- The discussion on required competences highlights that technical skills—such as cloud security, OT security, and incident response—are crucial, but only truly effective when combined with strong soft skills.
- In particular, the ability to translate technical risks into language that is understandable to other departments and management is essential.
- This requires professionals who can bridge the gap between technology and business objectives—the so-called T-shaped professionals.
- Soft skills such as communication, ethical awareness, and the ability to learn are therefore widely lacking but are indispensable for building bridges between IT teams and other parts of the organisation.

Focus group 2: Representatives in upper secondary education

Selection criteria participants:

- Currently teach IT-related subjects at secondary schools, vocational schools, or professional institutions for students aged 16–20
- Able to identify common cybersecurity risks and basic protective measures relevant to young learners
- Familiar with cybersecurity career pathways and how they are (or could be) represented within the curriculum
- Have experience with or responsibility for developing or implementing IT-related curricula at the secondary level
- Able to reflect on and discuss pedagogical strategies to enhance student engagement, skill development, and inclusivity in IT/cybersecurity topics

Part 1: implication cybersecurity trends for education
Based on your experience, how can education prepare and develop students (aged 16–20) in the competences that employers consider most important?

- Practical learning environments are essential to prepare students for the workplace. Participants stressed that theoretical instruction alone is not sufficient. Students should develop (practical) skills through applied tasks such as labs, realistic scenarios, and exposure to professional cybersecurity tools.

Co-funded by the European Union

- Cybersecurity is only marginally addressed in current secondary education curricula. Participants observed that relevant topics are offered inconsistently and often only superficially. There is a lack of structured and comprehensive programmes that treat cybersecurity as a core domain.
    - A participant pointed out: “We don’t have anything extra to offer for students in cybersecurity topics.”
- Education struggles to keep pace with rapid developments in cybersecurity and related technologies. Participants noted that technological innovation outpaces curriculum updates, leading to a mismatch between what is taught in schools and what is needed in the workplace. Limited access to modern tools and outdated materials further widens this gap.
- Students need early exposure to cybersecurity to discover their interest and develop intrinsic motivation. Participants emphasised that engaging students through projects, competitions, and exploratory activities helps them recognise their potential and drives deeper learning. This is especially important given the technical depth of cybersecurity and the personal commitment it often requires.
    - A participant mentioned: “Capture the Flag competitions are a great tool [...] it’s incredible how much they can learn when you give them the materials, the directions.”

Based on your experience in upper secondary education, what are some effective (didactic) approaches to make cybersecurity topics more relevant and engaging for students aged 16–20?

- Game-based and challenge-driven learning becomes even more effective when students collaborate or compete. Participants emphasised that cybersecurity concepts become more engaging when students are immersed in real-world scenarios through games, simulations, or escape rooms. Motivation increases further when activities involve teamwork, peer interaction, or friendly competition.
    - A participant mentioned: “Games and simulations are very important because they have the fun aspect and students love them.”
- Embedding cybersecurity activities within the curriculum increases participation and lowers motivational barriers. Participants noted that when projects or engaging activities are offered as optional, only highly motivated students benefit. Making them part of the standard timetable ensures broader exposure and supports students who may not self-select into the subject.
    - A participant suggested: “One year, I would make it mandatory. Then, if they want more, I would give them the option.”

Which specific topics, teaching formats or examples have you seen effectively spark students’ interest in cybersecurity?

- Students are most engaged when they recognise the personal relevance of cybersecurity and apply it through creative, hands-on projects. Participants noted that realistic examples (e.g. phishing, scams) capture attention, while project-based learning, like building password tools or games, helps internalise key concepts

Co-funded by the European Union

What barriers do educators face when trying to implement these engaging approaches in the classroom?

- Teachers face significant structural and practical barriers, and the degree of curricular freedom varies between schools. Participants indicated that national curricula offer some degree of flexibility in how cybersecurity is taught. However, limitations in time, funding, equipment, and the need for administrative approval often hinder the implementation of hands-on or gamified approaches.
    - A participant stressed: "I'm not paid extra for it. It's basically my goodwill."

Based on your experience in upper secondary education, what are the barriers that prevent young women from engaging with cybersecurity topics or considering related careers?

- Stereotypes and social dynamics can hold girls back from exploring cybersecurity, even when they have the skills. Participants explained that girls often internalise the idea that IT is a "boy's field", leading to hesitation, lack of confidence, or passive behaviour in mixed settings. These patterns are reinforced by peer expectations and classroom group dynamics. Teachers noted that even skilled girls may avoid programming or wait for others to take the lead.
    - A participant highlighted: "All of the boys gathered eagerly around the table, taking the lead in dismantling the monitor. Meanwhile, the girls stood at a distance, observing but not engaging. Hesitant to step in, even though they were just as capable."

Based on your experience in upper secondary education, what are the barriers that prevent young women from engaging with cybersecurity topics or considering related careers?

- When cybersecurity is framed narrowly as programming, it excludes those more interested in ethical, communicative, or creative aspects. Participants emphasised that girls often respond more positively to educational, design, or law-related cybersecurity topics. Broadening the scope and showing interdisciplinary applications makes the field more approachable.
- Without seeing women in cybersecurity roles, girls may not view it as a realistic or welcoming path. Participants highlighted the importance of showcasing female professionals and increasing visibility of women in teaching and career settings. Representation helps normalise women's presence in the field and inspires students to envision themselves in similar roles.
    - A participant highlighted: "In our school we had a career day with some professionals, but there were no professional women talking about their jobs."

What changes or additions to the curriculum could make cybersecurity more appealing or accessible to young women?

- Linking cybersecurity to relatable and interdisciplinary topics can broaden its appeal to girls. Participants suggested that connecting cybersecurity to themes like social media, communication, law, and ethics makes it more accessible and interesting. This is especially interesting to students who may not be drawn to the technical or programming side. This helps break the stereotype that cybersecurity is only for "tech-savvy" students.

Co-funded by the European Union

- Start cybersecurity education earlier and use active learning to keep girls engaged. Participants suggested that schools should introduce cybersecurity topics before students make final subject or career choices. Hands-on methods can help students stay engaged. These approaches are especially helpful for girls. They support confidence-building, even for students who are not interested in programming.

Part 2: conclusions

- Cybersecurity education must start earlier, go deeper, and focus more on hands-on skills.
- In most upper secondary education programmes, cybersecurity is only addressed briefly and superficially, leaving students without practical knowledge and experience.
- In addition, outdated curricula struggle to keep pace with fast-changing technologies, which means students rarely gain access to modern tools or realistic learning environments.
- As a result, students lack early exposure through projects and competitions that could help them discover their interest and develop relevant skills in cybersecurity.
- Such active, applied learning experiences contribute not only to the development of students' technical ability but also strengthen their intrinsic motivation.
- Engagement rises when students can relate cybersecurity to their daily lives.
- Student motivation improves when cybersecurity is taught through active formats like games, simulations, and real-life problem-solving.
- Especially when tasks focus on everyday digital habits, like securing Wi-Fi, detecting phishing, or creating strong passwords, students are more likely to understand the relevance.
- These practical approaches boost both confidence and ownership, even among students who are not initially drawn to technical topics.
- By connecting cybersecurity to their personal experience, educators create space for deeper learning and sustained engagement.
- Girls tend to hold back in cybersecurity classes, unless the subject is broadened.
- During group assignments, girls often adopt a cautious, passive attitude, even when they have the necessary skills and knowledge.
- This dynamic shifts when cybersecurity is linked to other domains such as communication, education, or social media.
- Projects that involve informing peers or addressing social issues visibly increase girls' sense of ownership and engagement.
- By presenting cybersecurity more broadly and allowing space for diverse roles and talents, more girls can see themselves reflected in the field.

Co-funded by the European Union

Focus group 3: Representatives in higher education

Selection criteria participants:

- Teaches IT or Computer Science subjects at a university or university of applied sciences, typically for students aged 18+
- Understands common cybersecurity risks and protective measures, and can contextualise these within higher education curricula
- Has knowledge of the cybersecurity labour market and career pathways, and understands how these can be aligned with advanced academic programmes
- Applies pedagogical methods that foster deep digital competences, inclusivity, and student engagement in IT and cybersecurity at tertiary level
- Is familiar with ECSF roles and e-CF ICT competences, and is able to integrate these into course and programme design in higher education.

Part 1: implication cybersecurity trends for education
Based on your experience, how can education prepare and develop students in the competences that employers consider most important?

- Foundational knowledge is the key to effective practical training. Participants emphasised that hands-on formats such as 'Capture the Flag' and virtual labs only deliver meaningful learning when built on solid theoretical foundations, yet this foundational content is increasingly being neglected. Without deep understanding of topics like DNS, protocols and cryptography, practical training becomes superficial and disconnected from the real demands of cybersecurity roles.
    - A participant stressed: "Hackathons are great, but not at the expense of the basics." and another participant added: "Students want to do CTFs in their free time, and it makes them enthusiastic… but our responsibility is to give them basic knowledge."
- Qualification frameworks hinder timely curriculum renewal. Participants emphasised that educators are bound by national qualification frameworks that change far too slowly to match the pace of technological developments and evolving job roles. This creates a vicious cycle: outdated standards lead to outdated courses, which in turn widen the gap with industry, at a moment when cybersecurity advancements are rapidly gaining speed and complexity.

What does it look like when a student is well-prepared for the workplace, in your experience?

- Balanced competences define true workplace readiness. Participants emphasised that success in cybersecurity depends not just on strong theoretical knowledge or hands-on ability, but on the integration of both. National education systems, however, often lean heavily in one direction: Dutch students are typically well-trained in practical assignments and soft skills, while Greek students often develop strong technical foundations but receive less emphasis on communication and presentation. This contrast shows that students need both technical understanding and the ability to communicate their ideas clearly, otherwise they may struggle in the professional field.

Co-funded by the European Union

- A participant mentioned: “There’s a huge difference in students that I get from all over Europe… in what their basic knowledge is and where the emphasis in their education has been.” and another participant added: “In Greece, students sometimes cannot even read the sentences they wrote in their own presentations.”

Based on your experience in higher education, what are some effective (didactic) approaches to make cybersecurity topics more relevant and engaging for students?

- Practice-based learning works best when it’s social, physical and active. Students are most engaged when they work together on real-world assignments in a shared physical environment, such as dedicated labs or project spaces. Being present on-site fosters informal peer learning, deeper interaction and hands-on experience that closely mirrors how cybersecurity teams operate in practice.
    - A participant mentioned: ”We ask students to commit to being present every day… we believe they learn from each other.” and added “We teach for two hours, and the rest of the day is labs. They learn a lot from each other.”

Based on your experience in higher education, what are some effective (didactic) approaches to make cybersecurity topics more relevant and engaging for students?

- Giving students ownership boosts relevance and motivation. Participants emphasised that students become more engaged when they actively shape the content and direction of their learning, often through flipped classroom formats. By researching topics, designing small experiments, and teaching peers, students build deeper understanding and take greater responsibility for their learning process.
    - A participant explained: “We have a flipped classroom where I give a short intro… then they divide the topic and present experiments to each other the next week.”

Which specific topics, teaching formats or examples have you seen effectively spark students’ interest in cybersecurity?

- Controversial or ‘grey area’ topics provoke strong engagement. Participants noted that themes such as hacker culture, ethics, cybercrime and grey hat practices tend to spark deep interest and vivid classroom discussions. Because these topics challenge moral boundaries and mirror real-world dilemmas, students become more emotionally invested and intellectually curious, often leading to lasting engagement.
    - A participant mentioned: “I just play devil’s advocate and try to do something that’s against the group—that really gets the discussion going.”

What barriers do educators face when trying to implement these engaging approaches in the classroom?

- Innovative teaching needs dedicated spaces—yet they’re often missing. Participants stressed that active, hands-on teaching approaches—like labs, group projects, and real-world simulations—depend on stable and well-equipped learning spaces. In practice, these are hard to secure: universities often prioritise flexible room use and efficiency, making it difficult for educators to claim or keep the physical spaces their teaching needs.

Co-funded by the European Union

- A participant stressed: “University planning hates this. They prefer sending students home—we constantly fight to keep our rooms.”

Based on your experience in higher education, what are the barriers that prevent young women from engaging with cybersecurity topics or considering related careers?

- Women want to belong, without being the focus. Many participants noted that female students in cybersecurity prefer not to receive extra attention or support just because of their gender. What they value most is being seen and respected for their skills, like any other student. The challenge is not in the subject matter, but in creating a culture where they feel equally included without being treated differently.
    - A participant indicated: “None of the stimulation programmes were perceived as positive by the women who studied with us.”
- Seeing women in cybersecurity makes a difference. Participants agreed that role models help normalise women’s presence in cybersecurity. Having female teachers or guest speakers shows young women that they belong. Even if they don’t ask for special attention, simply seeing others like them succeed can make a lasting impression.
    - A participant mentioned: “We have a female teacher for networking—it’s very hard to find them, but it really makes a difference.”

What changes or additions to the curriculum could make cybersecurity more appealing or accessible to young women?

- Context matters: gender imbalance is seen differently across countries.
- Participants observed stark differences in how the gender gap in cybersecurity is perceived across Europe. In countries like Croatia or Cyprus, educators reported a balanced male–female ratio and saw little need for targeted interventions. They emphasised that women who are interested simply join and succeed without facing visible barriers.
- In contrast, Dutch participants described a more pressing imbalance, especially in technical programmes where male dominance can be as high as 90%. They noted that decades of national efforts had little long-term effect and pointed to deep-rooted cultural and socioeconomic factors, such as parental expectations and career stereotypes.
- While most participants agreed the issue isn’t caused by curriculum content, they did acknowledge that visibility, inclusion, and broader STEM policy still play a role in making women feel welcome.

Part 2: conclusions

- Without solid theory, practical training falls short.
- Cybersecurity education should not focus too much on ‘fun’, hands-on activities like hacking games or simulations if students don’t first understand the basics.
- Without a clear grasp of core topics like DNS, cryptography or network protocols, practical exercises may feel exciting, but students may struggle to fully understand what they're doing or why it matters.

Co-funded by the European Union

- Educators should see theoretical knowledge as the starting point, not a hurdle, because it gives students the tools, they need to make sense of what they do in practice and succeed in the professional field
- Active learning only works when the right conditions are in place
- Students become more motivated when they work together on real problems in a shared physical space through labs, projects or flipped classrooms.
- These settings help them take ownership, learn from peers, and gain hands-on experience that feels relevant and real.
- But this kind of learning depends on having stable, dedicated spaces, something universities don't always prioritise, making it harder to offer the depth and continuity that active formats require.
- To truly unlock the value of these approaches, institutions must ensure the right conditions are in place (physical spaces, time, and continuity), so that practice-based learning can thrive.
- Belonging matters more than special treatment
- Across Europe, perceptions of gender in cybersecurity differ sharply: while educators in Croatia or Cyprus see little imbalance, Dutch participants report persistent underrepresentation of women, despite years of national efforts.
- What female students value most, however, seems consistent: they want to be respected for their knowledge, not highlighted for their gender.
- Creating a sense of belonging means more than adjusting the curriculum.
- It takes a shared effort from schools, policymakers, and employers to show that women naturally belong in cybersecurity, without making a big deal out of it.

Co-funded by the European Union

Annex 8 ECSF roles

To read the summarised recommendations and suggestions for new roles, please refer to 3.4 'Adjustments to and creation of ECSF roles'. This annex provides the detailed analysis and data collection.

1. Chief Information Security Officer (CISO)

The current definition of the Chief Information Security Officer (CISO) states: "Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected" (ENISA, 2022). Using the aforementioned dual analysis approach, employing both match-based and name-match approaches, reveals minor gaps and misalignments between this ECSF role's definition and labour market demands.

1.1. Match-Based Approach

The match-based analysis reveals that only 4 out of 7 evaluated vacancies align to a lower extent (40%) with the current ECSF CISO role, with none of these matches representing the highest observed compatibility score (60%). This indicates a considerable mismatch between the vacancies found in the labour markets and the ECSF role.

1.2. Name-Match Approach

The more focused name-match approach allowed the collection of 16 CISO vacancy postings. The listing of these vacancies and their assigned competences visualise the gaps between the currently assigned ECSF competences and the vacancies more precisely.
The key observations are:

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A7 (Technology Trend Monitoring)			0	0	0	The CISO position requires a holistic overview on technology trends, making the dismissal of this competence from this role not recommendable, despite seeming misalignment.
D1 (Information Security Strategy Development)				4	1	This suggests a higher demand for adjusting existing information security strategies rather than leading the development of new ones, indicating the focus of companies and institutions to learn and take over best practices from the wider market rather than developing new standards and approaches internally.
E3 (Risk Management)		1	1	4		High demand met with accuracy of the definitional competence level. This underlines the accuracy of the assigned competence.
E8 (Information Security Management)		0	2	8		This shows that while operational tasks are demanded, more often strategic leadership is demanded in CISO vacancies.
E9 (Information Systems Governance)				2	1	Demand visible, dataset too low to determine whether competence level is set too high.

Co-funded by the European Union

1.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A1(Information Systems and Business Strategy Alignment)				1	4	Emphasises demand for strategic leadership in solution development and interdepartmental support. This competence is not currently required by any ECSF role yet aligns closely with CISO responsibilities.
D3 (Education and Training Provision)		1	5			Concerns staff training and labour market awareness, peripheral but relevant to CISO vacancies focused on organisational readiness.
E6 (Quality Management and Compliance)		0	2	4		Demand for quality assurance leadership by employees in the CISO position, relevant information but more indirectly related to the role's defined tasks.

1.4. Recommendations for ECSF Role Enhancement

To improve alignment between ECSF-defined roles and competency demands in the labour markets, the following changes are recommended:

- Changing the E8 competence level requirements from e3 to e4, matching market demand whilst aligning to ECSF role definitions.
- Inclusion of A1 (e5) in the CISO competence set:
  - High market demand and no overlap with other ECSF roles make this a compelling candidate for addition.

1.5. Consideration of a new role

Alternatively, instead of adding the competence A1 (Information Systems and Business Strategy Alignment) to the definitional competence list of the CISO role, it is worth considering to develop a new ECSF role which fills a gap left by the CISO role and other ECSF roles. Due to the visibly high demand for the competence D1 (Information Security Strategy Development) as well as high demands in the unassigned A1 (Information Systems and Business Strategy Alignment), E6 (Quality Management and Compliance) and D3 (Education and Training Provision), the suggestion can be made to create an ECSF role which decreases the near all-encompassing task-range of a CISO and take-up lower priority tasks, which on one hand supports the CISO role and organisational readiness whilst on the other hands prepares the employee for filling up the CISO role, once it becomes vacant. It would thus act as a bridging position, which prepares the employee for the CISO role and includes demanded technical as well as 'low-level' executive tasks. A suggestable title which would encompass these tasks and represent the position's level, would be *Security Governance Manager* but this can also be seen as an Information Security Officer (ISO) or -Manager, a role that has been described in e-CF amongst other.

Co-funded by the European Union

2. Cyber Incident Responder

The Cyber Incident Responder, as defined in the ECSF, monitors the organisation's cybersecurity state, handle incidents during cyber-attacks and assure the continued operations of ICT systems (ENISA, 2022). The findings from both the match-percentage and task-based analyses highlight mismatches between the ECSF competence assignments and current market demands.

2.1. Match-Based Approach

Among the five evaluated vacancies, three achieved a match score of 40%, with no higher alignment detected. This suggests limited coherence between the current ECSF Cyber Incident Responder role definition and the scope of responsibilities outlined in the used vacancy postings.

2.2. Name & Task Range Approach

The analysis of competences based on 10 Incident Responder vacancies currently assigned to the Cyber Incident Responder role revealed several key insights:

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A7 (Technology Trend Monitoring)			1	1	1	Competence demanded on all levels, insufficient data to identify demand patterns.
B2 (Component Integration)		0	0	0		Lack of data suggests low demand for this competence.
B3 (Testing)	0	1	0	0		Lack of data suggests low demand for this competence.
B5 (Documentation production)	1	0	0			Lack of data suggests low demand for this competence.
C4 (Problem management)		2	3	1		The mismatch in demand levels suggests that the assigned e4 level for C4 may be set too high. Adjusting this to e3 would align more closely with vacancy requirements, without undermining the role.

2.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
D1 (Information Security Strategy Development)				3	0	Highlights that strategic leadership is not typically expected from Incident Responders, they are more often expected to focus on developing operational best practices.
D12 (Security Consulting)			1	3		This competence appears broadly across many vacancy types in the dataset. Its general nature and frequency reduce its value for this specific role and therefore its inclusion is not recommended.

Co-funded by the European Union

2.4. Conclusion & recommendations

The current ECSF Cyber Incident Responder role captures several key functions but shows misalignment in competence levels and an incomplete reflection of market demands. The dataset suggests a lowering of the C4 competence level from e4 to e3 to improve alignment to Cyber Incident Responder vacancies found in current labour markets. Additionally, D1 appears more frequently in vacancies related to this ECSF role, indicating a more general demand for Incident Responders to develop operational best practices. Its addition on level 4 is cautiously recommended. However, the addition of D12 is not recommended due to its broad applicability and very frequent demand across all vacancies found in the entire dataset.

3. Cyber Legal, Policy & Compliance Officer

The current ECSF definition of the Cyber Legal, Policy & Compliance Officer (CLPCO) states: "Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organisation's strategy and legal requirements" (ENISA, 2022). This includes oversight of compliance testing, policy development, and communication with stakeholders.

3.1. Match-Based Approach

The match-based analysis includes five relevant job postings, of which four align to varying extents with the current ECSF CLPCO definition. Notably, two postings match at a 75% level, fulfilling nearly all required ECSF competences and their levels. These high matches confirm the general robustness of the ECSF role definition. The other two postings score at a 50% match, indicating some deviations but still suggesting substantial alignment.

3.2. Name-Match Approach

A more granular name-match analysis supports and refines the above observations. The following ECSF-assigned competences were identified in the 11 reviewed CLPCO vacancy postings:

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A1 (Information Systems and Business Strategy Alignment)				1	0	Reflecting the need for strategic understanding of information systems and business alignment, though not prominently demanded.
D1(Information Security Strategy Development)				0	0	Surprisingly absent, despite its relevance to information security strategy; this suggests employers may implicitly assume strategic input rather than requiring it explicitly.
E8 (Information Security Management)		0	1	0		Demand does exist; however, data does not permit the determination of patterns, allowing in turn to formulate sound advice.
E9 (Information Systems Governance)				1	0	Data indicates demand on the level defined by the ECSF role; data is too sparce to make it a definite conclusion however.

Co-funded by the European Union

3.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
D7 (Science and Data Analysis)		0	2	2	0	The overall demand is too fragmented and sparse to warrant inclusion in the standard ECSF profile.
E4 (Relationship management)			2	2		Appears with moderate consistency, but the evidence base is limited and not strong enough to recommend its formal assignment to this role.

3.4. Consideration of a New Role

Although not included in the above demonstrated dataset, reviewing the vacancy descriptions, an underlying demand for documentation becomes apparent. Considering the fast-paced development of international, EU-wide legislation such as NIS2/DORA/CRA, it is worth considering a complementary ECSF role to the CLPCO that focuses on evidence collection and the tracing of regulatory changes. A role which would envelop these tasks would be the *Compliance Officer*. However, due to limited supporting data at this point and risk of fragmentation of the CLPCO role, a new role should only be introduced once labour market demands become too intense for the CLPCO to cover these tasks.

3.5. Conclusion & recommendations

Although data is sparce and too minimal to identify well founded patterns, the existing data does point at well placed competences and their levels. This and the fact that demand for other competences in the labour market is too dispersed to identify patterns which would warrant adjustments for this ECSF role no recommendations for this role can be made at this time. Nonetheless, when paying attention to the vacancy descriptions, a trend can be identified which warrants the recommendation to start considering a new ECSF role, which resembles the one suggested above.

4. Cyber Threat Intelligence Specialist

The ECSF defines the Cyber Threat Intelligence Specialist as a technically focused role responsible for the collection, evaluation, and analysis of threat-related information to produce actionable intelligence reports and disseminate them to target stakeholders (ENISA, 2022).

4.1. Match-Based Approach

This analysis covers seven threat intelligence-related vacancies, of which four show alignment and three do not. All matched vacancies reach only a 40% compatibility rate, suggesting that even aligned vacancies only partially reflect the ECSF roles currently assigned competences. The competences E.4 (Relationship Management) and E.8 (Information Security Management) appear most consistently, though even their representation is inconsistent across postings.

Co-funded by the European Union

The scattered presence of key competences and the absence of high match scores across the board suggest that the labour market defines the role more variably than the ECSF role can currently represent, potentially reflecting emerging or hybrid functions.

4.2. Name-Match Approach

The analysis of 14 Threat Intelligence Specialist vacancy postings offers a deeper view into the competences required by employers for Cyber Threat Intelligence Specialists. The following ECSF-assigned competences were found:

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
B5 (Documentation Production)	0	0	2			While present, this competence appears infrequently and at lower levels, indicating a supporting rather than central function, which is further underlined by the vacancies' descriptions.
D7 (Science and Analysis)		0	1	4	0	A strongly prioritised and frequently requested skill, reflecting strong analytical expectations across threat intelligence functions.
D10 (Information and Knowledge Management)			0	1	0	Although being a key ECSF competence for this role, demand appears low. Upon reviewing the vacancy description, demand for this competence is higher than originally categorised.
E4 (Relationship Management)			1	1		Demonstrates, together with vacancy descriptions, moderate demand for stakeholder and interdepartmental collaboration, although inconsistently.
E8 (Information Security Management)		0	0	0		Surprisingly absent, considering its theoretical relevance to managing threat mitigation processes. Upon revisiting the vacancies' descriptions this competence is highly demanded, although more often implied by context.

4.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A7 (Technology Trend Monitoring)			1	3	0	Data suggests employers expect threat intelligence specialists to remain current with technological developments and build early-warning capabilities around emerging threats. However, A7 is already shared across several ECSF roles, and its inclusion here would risk blurring role boundaries despite its contextual relevance.

Co-funded by the European Union

A9 (Innovating)				3	0	This competence supports the demand for creative threat response strategies and evolving analytic methodologies. However, its broad nature makes it unsuitable for formal inclusion without clearer market consensus or more explicit role differentiation.

Although the apparent inconsistency in labour market demands upon reviewing vacancy descriptions, no adjustments are recommended at this stage as vacancy-ECSF role-alignment is higher than the data suggests.

4.4. Consideration of a New Role

Based on the analysis of the vacancy description, it becomes noticeable that the vacancies connected to the Cyber Threat Intelligence Specialist role base on more reactive activities, whilst a pro-active role may be of future interest. Such a role would then require specifically the competences of A9 (Innovation), as well as A7 (Technology Trend Monitoring), compounding to a more strategic and forward-looking responsibility range, creating a role such as the *Threat Innovation Analyst*.
Yet again, the current lack of structured market data makes this a premature move, warranting further monitoring and validation before considering its development and implementation. Nonetheless, trends and demands do point towards a likely future need for such a position.

4.5. Conclusion & recommendations

The Cyber Threat Intelligence Specialist role, as currently defined in the ECSF, captures some of the demanded responsibilities. The frequent demand for D.7 (e4) confirms the relevance of the competence for this role, while competences such as D.10 and E.8 appear less demanded on the market. Labour market trends increasingly emphasise trend awareness and innovative thinking, yet the competences supporting these functions (A7, A9) are too broadly shared across other roles to recommend their inclusion without clearer boundaries. The fragmented nature of market's expectations points to an evolving role, potentially requiring either future ECSF updates or the creation of a specialised innovation-focused intelligence track. For now, no refinements to competence levels are required to bring the ECSF role into closer alignment with actual labour market demand.

5. Cybersecurity Architect

The ECSF Cybersecurity Architect "plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls" (ENISA, 2022).

5.1. Match-Based Approach

Out of five matching and evaluated vacancies, four demonstrate alignment with the ECSF-defined Cybersecurity Architect role, indicating a generally sound role definition. One vacancy shows a strong compatibility score of 80%, while the others range between 40% and 60%. This suggests that while the ECSF framework broadly captures the core functions of the Cybersecurity Architect, minor variability exists in labour market demands.

5.2. Name-Match Approach

The analysis of 24 vacancies for their assigned competences, highlights several alignment trends and gaps:

Co-funded by the European Union

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A5 (Architecture Design)			3	0	0	Higher demand for determining best practices in IT infrastructure instead of leading the implementation organisation-wide strategies.
A6 (Application / Product Design)	0	0	1			Lack of matches is underlined by the low focus given in the vacancy descriptions. This remains a relevant and demanded competence however.
B1 (Application / Product Development)	0	1	4			Underlines the correct representation of current labour market needs.
B3 (Testing)	0	0	0	0		Testing is not demanded in the analysed vacancies, indicating that this task is being demanded dedicated attention, which for example may be conducted by Pen testers.
B6 (ICT Systems Engineering)			2	0		The data suggests that there is higher demand for operability and direct solving of issues rather than the broad, strategic approach for a company's IT architecture. This however cannot be conclusively stated, as the dataset remains too small.

5.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
C1 (Use Support)	0	3	0			Suggests demand that architects maintain awareness of user-centric support requirements and liaise with support teams or customers directly to ensure usability and secure deployment.
E.4 (Relationship Management)			2	5		This signals a rising demand for cross-departmental, institutional, and even inter-organisational collaboration in the secure architecture development process, an area underrepresented in the current ECSF role definition.

5.4. Recommendations for ECSF Role Enhancement

Firstly, the lack of matches is caused by a low assignment rate of competences to the individual vacancy, ranging from one competence per vacancy to 4. The above given notes are mostly formulated by re-evaluating the vacancy descriptions individually. Hence, to better align the ECSF Cybersecurity Architect role with labour market demands, the following refinements are proposed:

- Inclusion of E4 (Relationship Management) at e4 level:
  - Strong presence across vacancy postings underscores the importance of direct cooperation engagement in architecture roles.

Co-funded by the European Union

- At present, only the Threat Intelligence Specialist role includes this competence within the ECSF, despite its growing relevance across strategic and design-oriented cybersecurity positions.

- Re-evaluation of B3 (Testing):
  - Given its absence in all examined vacancies, consider removing B3 from the architect's core competence set to avoid misrepresentation of the role's practical focus.

5.5. Conclusion & recommendations

The ECSF Cybersecurity Architect role displays strong foundational alignment with market demands, as evidenced by high percentage match scores across vacancies. However, the role's current competence set underrepresents the increasingly collaborative nature of secure architecture development. The high frequency of E4 (Relationship Management) indicates a trend of blending technical design with organisational alignment and stakeholder coordination. Adjusting the ECSF framework to reflect these trends would enhance its accuracy, improve role-to-vacancy matching, and future-proof the role against continued market evolution.

6. Cybersecurity Auditor

The Cybersecurity Auditor is required to:" Perform cybersecurity audits on the organisation's ecosystem. Ensuring compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices" (ENISA, 2022).

6.1. Match-Based Approach

The analysis covers ten vacancy postings, yet only two demonstrate alignment with the ECSF-defined Cybersecurity Auditor role. Furthermore, the highest-matching vacancies do not align by title or description, while a vacancy explicitly titled *Senior IT Auditor* returns a 0% match with the ECSF-definitional competences. This points to discrepancies between ECSF's framing of the role and how the vacancy is advertised or how the competences are assigned to the vacancies.

6.2. Name-Match Approach

The name- and task-based analysis confirms a seemingly fragmented competence profile for 10 Cybersecurity Auditor postings. However, the assignment of competences to the vacancies shows again strong discrepancies, with some vacancies having one competence assigned, whilst others are assigned six. The variation appears to be driven largely by differences in job context, such as whether the auditor operates internally, externally, or in a purely consultive capacity. This diversity contributes, arguably, to the lack of coherent patterns across the assigned ECSF competences.

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
B3 (Testing)	0	0	0	0		Not observed at any level, including the vacancies' descriptions. Indicates a lack of demand for this competence in this role.

Co-funded by the European Union

B5 (Documentation Production)	0	0	0			The vacancy descriptions do not include the demand for documentation production verbatim, but implies it generally, indicating a low, but existing demand for this competence. The shown data is thus not representative.
E3 (Risk management)		1	1	0		Although occurring occasionally, the demand occurs in high-ranking vacancies but at lower competence levels. It should thus not be considered a major task and skill requirement of the auditor.
E6 (Quality Management and Compliance)		0	1	0		The vacancy descriptions do demand this competence more regularly than the data to the left suggests. The context of the text implies a high priority in this competence.
E8 (Information Security Management)		0	1	0		The data implies that the labour market demands auditors to evaluate and consult on improvements of security standards, not on leading their implementation on the company's strategic scale.

6.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
E4 (Relationship Management)			3	0		As several Auditor vacancies require the applicant to work for third parties, the demand for E4 can be explained.

6.4. Recommendations for ECSF Role Enhancement

At this stage, few specific changes to the ECSF Cybersecurity Auditor role are recommended. The following factors make the current data insufficient for well-founded recommendations:

- B3 (Testing): Should be reconsidered as a definitional competence of this ECSF role as none of the vacancies mention in any way the requirement of testing systems. Instead, it emphasises cooperation and evaluation, insinuating the cooperation with other positions in order to focus on the evaluation of compliances.
- E3 (Risk Management): Although demand can be found in the labour market, this competence is required at a low competence level for high-ranking auditor vacancies. The competence level 4 does thus not seem to be representative of labour market demands. It is recommended to lower the competence level from 4 to 3. 7. Cybersecurity Educator Role The Cybersecurity Educator role is focused on designing and delivering cybersecurity education and training, with responsibilities linked to personnel development, awareness creation, and skill-building within organisations (ENISA, 2022).

7. Cybersecurity Educator

The Cybersecurity Educator role is focused on designing and delivering cybersecurity education and training, with responsibilities linked to personnel development, awareness creation, and skill-building within organisations (ENISA, 2022).

Co-funded by the European Union

7.1. Match-Based Approach

Out of 11 analysed vacancies, only two show alignment with the ECSF Cybersecurity Educator role. This limited match is primarily driven by the frequent presence of D.3 (Education and Training Provision), which is widely assigned to other roles as well. Its high prevalence regardless of actual task alignment risks inflating false positives during role-to-vacancy mapping. A manual review revealed only one partial match among education-focused roles. The findings suggest that actual educator roles are often defined with narrower or different competences than those currently assigned to the ECSF Cybersecurity Educator profile.

7.2. Name-Match Approach

The name- and task-alignment analysis reveals key issues with the current competence assignment, with only limited coverage of defined competences set by the ECSF role. 11 vacancies were collected and analysed:

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
D3 (Education and Training Provision)		1	1			The data confirms this competence's relevance.
D9 (Personnel Development)		0	0	0		Not found in any of the 11 vacancies, raising doubts about its applicability. Its current definition appears to focus on internal staff development, which does not align with the externally focused, service-oriented nature of many real-world educator roles.
E8 (Information Security Management)		0	1	0		Unclear relevance in most educator contexts, as this competence focuses on reviewing and/or controlling IT system policies. Yet again it also focuses on the distribution of found knowledge to those of interest. A competence which does not clearly match the task demands found for vacancies matching this ECSF role.

7.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
B1 (Application/Product Development)	0	0	3			Indicates demand for educators who can design or maintain digital training platforms, e-learning systems, or instructional tools—suggesting a strong digital delivery focus.
D12 (Security Consulting)			3	3		Reflects market demand that educators act in advisory or consultative roles, especially when offering tailored training to clients or external stakeholders. Due to the broad demand for this competence however, it is not recommendable to add D12 to the definitional competence list of this ECSF role.

Co-funded by the European Union

These unassigned but recurring competences point toward an underrepresentation of key functional areas in the current ECSF role, namely the digitalisation of education.

7.4. Recommendations for ECSF Role Enhancement

Based on the analysis, several adjustments are recommended to improve the ECSF Cybersecurity Educator role's accuracy and relevance:

- Redefine or remove D9 (Personnel Development):
  - Current ECSF definition is interpreted heavily as internal staff development. Since the majority of observed vacancies are externally focused, this competence appears misaligned. The recommendation is thus: Either expand D9's definition to clearly include the development of external peers or clients or remove it from the Cybersecurity Educator profile.
- Include B1 (Application/Product Development) at e3 level:
  - Reflects widespread demand for educators to design and deliver digital learning content and platforms. This is in line with the visible trend of the shift toward e-learning and hybrid training models.

8. Cybersecurity Implementer

The Cybersecurity Implementer "develops, deploys and operates cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products" (ENISA, 2022).

8.1. Match-Based Approach

From eight analysed vacancies, five align with the ECSF-defined Cybersecurity Implementer role. Notably, one vacancy reaches an 80% compatibility score, while others achieve 60% and 40% matches, respectively. These results suggest a high demand for this role across the labour market and a solid ECSF definition that broadly captures its core responsibilities.

8.2. Name-Match Approach

The name- and task-range match further supports the view that the ECSF Cybersecurity Implementer role captures core responsibilities, however missing some high demand competences that appear in real-world job postings. It is important to note, that this dataset has a particularly large number of vacancies, totalling 94, coinciding with the Implementer role, underlining the labour markets' demand for this role and its task range.

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A5 (Architecture Design)			14	6	3	Strong presence suggests implementers are often expected to contribute to design discussions, especially in agile or DevOps settings.
A6 (Application / Product Design)	0	1	5			Emphasises market demand for technical adaptability.
B1 (Application / Product Development)	1	4	8			Consistently present, showing implementers' involvement in system building and deployment.

Co-funded by the European Union

B3 (Testing)	1	6	11	0		Underlines that system validation is a key part of the role and highly demanded on the market.
B6 (ICT Systems Engineering)			8	6		Strong presence underlines the alignment of the ECSF role definition with current labour market demand.

8.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
C4 (Problem Management)	2	8	7			Data demonstrates high market demand for this competence in the implementer role. However, demand for this competence is not high enough to suggest inclusion in recommendations.
C5 (Systems Management)		8	15	2		Shows that system oversight and operational responsibility are common expectations for this role.
B5 (Documentation Production)	2	9	13			Generally high demand, by reviewing the vacancy description however, this competence is of low priority and thus insufficiently strong to recommend its inclusion into the definitional competence list of this ECSF role.

8.4. Recommendations for ECSF Role Enhancement

The ECSF Cybersecurity Implementer role is already well-defined and strongly aligned with labour market expectations. Nonetheless, based on found patterns in the data, the following addition to the roles definitional competence list is recommended:

- Include C5 (Systems Management) at e3 level:
  - Reflects widespread expectation for implementers to ensure the continuity, configuration, and monitoring of systems they help deploy.
  - Enhances the ECSF's ability to differentiate between purely developmental and operational cybersecurity roles.

9. Cybersecurity Researcher

The Cybersecurity Researcher is dedicated to "research the cybersecurity domain and incorporate results in cybersecurity solutions" (ENISA, 2022).

9.1. Match-Based Approach

Out of seven analysed vacancies, four align with the ECSF-defined Cybersecurity Researcher role, while three do not. Interestingly, both matching and non-matching vacancies report similar compatibility scores (40%), but non-matching roles show a broader spread of assigned competences (6–13) compared to 3–5 for the aligned roles. This suggests that roles with broader task scopes may create artificial overlaps across ECSF roles during automated mapping. Notably, the competences A.7 (Technology Trend Monitoring) and A.9 (Innovating) are considered core to the ECSF Researcher profile and are defined at e5 level, yet neither appears at that level in any analysed vacancy. Instead, these competences appear at lower levels (e3–

Co-funded by the European Union

e4), indicating that the market favours a less senior or less strategic interpretation of these research functions than ECSF currently assumes.

9.2. Name-Match Approach. The analysis reveals that the 11 found researcher vacancies prioritise analytical and collaborative functions over operational or hands-on problem resolution.

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A7 (Technology Trend Monitoring)			0	2	0	Never demanded at the expected e5 level. Although demand can be found.
A9 (Innovating)				1	0	Never demanded at the expected e5 level. Although demand can be found.
C4 (Problem Management)		0	0	0	0	Not matched at all, suggesting that researchers are not expected to resolve operational issues, but instead to focus on procedural or analytical outputs.
D7 (Science and Analysis)		1	2	1	0	Data confirms the core analytical orientation of the role.
D10 (Information and Knowledge Management)			0	1	0	Underreported due to implicit task descriptions in vacancy texts, making competence assignment inconsistent.

9.3. Unassigned but noteworthy Competences

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
D9 (Personnel Development)		0	3	0		Data points at the expectation that researchers contribute to developing others' knowledge, especially in collaborative or mentoring environments. This is underlined by several vacancy descriptions used in this dataset.
E4 (Relationship Management)			1	3		Data is indicating a need for external engagement of researchers, including sharing insights with third parties, clients, or the broader security community.

These patterns reveal that researchers are increasingly viewed as knowledge-sharing facilitators, whose success is measured not by direct problem resolution, but by their ability to generate, communicate, and diffuse knowledge.

9.4. Recommendations for ECSF Role Enhancement

The current ECSF definition for the Cybersecurity Researcher role would benefit from a targeted refinement to better reflect actual labour market expectations:

Co-funded by the European Union

- Consider removing C4 (Problem Management):
  - Not matched in any analysed vacancy, suggesting a misalignment.
  - Researchers are regarded not to be operational troubleshooters, but rather analysts and communicators.
- Consider adding E4 (Relationship Management) at e4 level:
  - Reflects the role's increasing involvement in external knowledge dissemination, networking, and collaboration.
- Consider adding D9 (Personnel Development) at e3 level:
  - Captures the role's contribution to internal and peer knowledge enhancement, especially in academic or think-tank environments.
- Adjust competence levels of A7 and A9:
  - Market demands these at e4, not e5. Lowering required levels would align ECSF expectations with labour market expectations for researcher roles and enable more accurate vacancy-role mapping.

10. Cybersecurity Risk Manager

The Cybersecurity Risk Manager "manages the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports" (ENISA, 2022). The role is designed to provide oversight over security-related risks, driving improvements in business continuity, governance, and resilience. Based on the current vacancy analysis, the ECSF role largely reflects core market expectations, but shows a few emerging trends, particularly in documentation, analysis, and governance, that may warrant a cautious adjustment of its competence set.

10.1. Match-Based Approach

Among the seven analysed vacancies, five align with the ECSF Cybersecurity Risk Manager role, while two do not. This suggests a strong general alignment between the ECSF role definition and real-world labour market expectations. Core assigned competences such as E.5 (Process Improvement) at e3 and E.7 (Business Change Management) at e4 appear with moderate consistency, while E.9 (Information Systems Governance), although central to the ECSF role, is less frequently demanded in the data.

10.2. Name-Match Approach

This approach highlights some clear patterns around governance and documentation tasks within the risk manager role. Assigned competences show partial alignment, while unassigned competences capture some additional, recurring expectations. A total of 16 Risk Manager vacancies have been analysed, finding the following:

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
E3 (Risk Management)		1	1	1		Data confirms accurateness of the competence in relation to this ECSF role.
E5 (Process Improvement)			2	0		Data confirms accurateness of the competence in relation to this ECSF role.

Co-funded by the European Union

E7 (Business Change Management)			0	2	0	Data confirms accurateness of the competence in relation to this ECSF role.
E9 (Information Systems Governance)				1	0	Data confirms accurateness of the competence in relation to this ECSF role.

10.3. Unassigned but noteworthy Competence

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
B5 (Documentation Production)	1	4	0			High demand for tasks like writing risk reports, analysis protocols, or audit documentation.

10.4. Recommendations for ECSF Role Enhancement

The Cybersecurity Risk Manager role is well-defined and well-aligned with labour market expectations. However, subtle shifts in vacancy data suggest that the ECSF competence profile could be modestly expanded for improved realism and analytical precision.
Suggested Adjustments:

- Consider adding B5 (Documentation Production) at e2 level:
  - Strong support in market data.
  - Enhances representation of the Risk Manager's involvement in evidence creation, formal reporting, and protocol development.

11. Digital Forensics Investigator

The Digital Forensics Investigator is assigned the task to "ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity" (ENISA, 2022). Current labour market data reveals inconsistencies between the ECSF role definition and vacancy demands, particularly around testing and analytical responsibilities.

11.1. Match-Based Approach

Out of seven analysed vacancies, only two align with the ECSF Digital Forensics Investigator role. Three vacancies show 50% compatibility, while the remaining four match at just 25%, indicating a low to moderate overall alignment with ECSF's current role formulation.
A key finding is the absence of B3 (Testing) in these vacancies—not only at the defined e4 level but across all competence levels, suggesting that this competence may be insufficiently suited to the actual tasks performed by forensics professionals in practice. In contrast, B5 (Documentation Production) shows more frequent matches, particularly when lower competence levels are included, highlighting the importance of procedural clarity, evidence documentation, and report writing.

11.2. Name-Match Approach

A deeper analysis of task descriptions and named competences provides insight into emerging labour market expectations that are not currently captured in the ECSF role definition. A total of 10 Forensic Investigator vacancies have been analysed:

Co-funded by the European Union

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
A7 (Technology Trend Monitoring)			0	2	0	Data confirms market expectation for forensic experts to utilise newest knowledge on emerging technologies and evolving cybercrime tactics instead of just analysing and reporting on it.
B3 (Testing)	0	2	1	0		Reviewing the vacancy description testing appears a minor task of the forensics' responsibilities. It is recommendable to lower the definitional competence level to 3.
B5 (Documentation Production)	0	0	1			While infrequent, its presence suggests forensic professionals are expected to generate procedural documentation, a task central to legal and investigative integrity.
E3 (Risk Management)		0	0	0		Surprisingly absent from all vacancies, despite being assigned to the ECSF role. This may indicate that forensic roles are operational rather than strategic, with risk functions often performed by other roles (e.g., Risk Manager or CISO).

11.3. Unassigned but noteworthy Competence

Competence	Competence levels (**green** = level suggested to be assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
D7 (Science and Analysis)		0	1	3	1	It aligns well with forensic investigators' analytical tasks such as evidence correlation, pattern detection, hypothesis formation, and reporting findings for legal or compliance purposes.

These findings strongly suggest that D7 is valuable to the actual practice of digital forensics, particularly at e4, which implies ownership of analytical processes and independent investigative responsibilities.

11.4. Recommendations for ECSF Role Enhancement

The current ECSF definition for the Digital Forensics Investigator requires revision to improve alignment with vacancy realities, particularly in terms of analytical and testing-related responsibilities.

Recommended Changes:

- Lower B3 (Testing) competence level:
  - Due to a rather minor relevance and task range of this competence in the vacancy descriptions, it is recommendable to lower the competence level from 4 to 3.

Co-funded by the European Union

- Add D7 (Science and Analysis):
  - Strongly demanded across analysed vacancies. Reflects the centrality of investigative analysis, data interpretation, and structured reasoning within forensic workflows. It adds nuance and improves the realism of vacancy-to-role mapping. Suggested to implement the competence at competence level 3.

12. Penetration Tester

The Penetration Tester "assesses the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors" (ENISA, 2022). This role is characterised by a deep engagement with testing, component integration, and solution deployment activities. However, a close analysis of available vacancy data reveals issues in match reliability and competence attribution, despite strong name alignment.

12.1. Match-Based Approach

This analysis includes eleven vacancy postings, of which only two are categorised as coinciding with the ECSF Penetration Tester role. Notably, neither of the two matching roles scores above 0%, even though both titles and described task ranges clearly align with the ECSF definition. This discrepancy is largely explained by the reoccurring, very low number of assigned competences per vacancy: both coinciding vacancies were only tagged with three competences each, while the other vacancies show between eight and thirteen competences per vacancy. Vacancies show between eighvThis suggests that the absence of matches is not due to conceptual misalignment between the ECSF and the labour market, but rather a data quality issue—specifically, the under-tagging of vacancies, which distorts competence-based match calculations.

12.2. Name-Match Approach

Despite the low percentage match results, a review of the assigned competences regarding the 10 Penetration Tester vacancies, sheds some light on potential areas of alignment and misalignment:

Competence	Competence levels (**green** = level assigned to ECSF role competence)					Notes
	e1	e2	e3	e4	e5	
B2 (Component Integration)		0	0	0		The lack of matches can be explained by two factors: Firstly, the tasks are often described in regard to the services they need to provide, not how their work will be done, such as by component integration. The description focuses much more on the consultive and supporting aspects of the vacancies. Evaluators unfamiliar with the general tasks of a Pen Tester may thus not be aware of the need of this competence. Secondly, once again the competence attribution per vacancy is too low, ranging from 2 to 3 and one 4. This is too low to have competences reliably match the vacancy description. The data is thus sub-optimally evaluated.

Co-funded by the European Union

B3 (Testing)	1	1	1	0		The demand for testing is evident but appears to skew toward junior/mid-level activities, or simply not be expressed in a way that maps clearly to the higher competence levels.
B4 (Solution Deployment)	0	1	0			While arguably relevant to pen testing, it seems to be infrequently acknowledged during the data evaluation.
B5 (Documentation Production)	1	0	0			Also, by re-evaluating the vacancy descriptions, this competence appears a minor priority demand for Pen testers.
E3 (Risk Management)		1	0	0		Although risk awareness is critical in pen testing, the explicit attribution of this competence indicates a lower competence level, data is too scarce to make this finding conclusive though.

12.3. Unassigned but noteworthy Competence

No clear patterns emerge from unassigned competences in this dataset. This underlines the limitations affecting analytical reliability.

12.4. Recommendations for ECSF Role Enhancement

The current data does not support reliable recommendations to modify the ECSF Penetration Tester role at this time, due to:

- Extremely low competence attribution across the analysed vacancies.
- Low match scores despite correct naming, indicating issues rooted more in data inconsistency than role-definition gaps.

However, two issues should be noted for future reassessment:

- The lack of specific mention of OT/IoT and automated VA skills in the ECSF should be addressed, possibly through the creation of a sub-role or additional specialisation layer under the Penetration Tester category. Not enough data could be evaluated to propose a new specific ECSF-role however.

Co-funded by the European Union

REFERENCE LIST

ASD. (2024). Annual Cyber Threat Report. *

Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills framework. *Computers & Security, 151*(1), 1-10.

CADMUS. (2025a). *Objective and Mission*. Retrieved from https://cadmus-project.eu/the-project/.

CADMUS. (2025b). About CADMUS Project. Retrieved from https://cadmus-project.eu/.

CADMUS. (2025c). Work Packages and Project Timeline. Retrieved from https://cadmus-project.eu/project-timeline/.

Cedefop. (2020). *Vocational education and training Europe 1995-2035: Scenarios for European VET systems*. Publications Office of the European Union. Retrieved from https://www.cedefop.europa.eu/files/3083_en.pdf.

Cisco. (2024). Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette. *

CrowdStrike. (2025). 2025 Global Threat Report. *

CONCORDIA. (2020). Deliverable D1.2: 2nd Year Report on Designing and Developing an European Secure, Resilient and Trusted Ecosystem (ESRTE).

CyberSecPro. (2022a). D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse.

CyberSecPro. (2022b). D2.2 Blended CyberSecPro Technological Training Interactive Technologies and Academic Practice.

CyberSecPro. (2024). CyberHubs – Cybersecurity Skills Needs Analysis – Summary Report

CyberSecPro. (2024a). CyberHubs - Cybersecurity Skills Needs Analysis (Belgium).

CyberSecPro. (2024b). CyberHubs - Cybersecurity Skills Needs Analysis (Estonia).

CyberSecPro. (2024c). CyberHubs - Cybersecurity Skills Needs Analysis (Greece).

CyberSecPro. (2024d). CyberHubs - Cybersecurity Skills Needs Analysis (Hungary).

CyberSecPro. (2024e). CyberHubs - Cybersecurity Skills Needs Analysis (Lithuania).

CyberSecPro. (2024f). CyberHubs - Cybersecurity Skills Needs Analysis (Slovenia).

CyberSecPro. (2024g). CyberHubs - Cybersecurity Skills Needs Analysis (Spain).

CyberSecPro. (2024h). CyberHubs - Cybersecurity Skills Needs Analysis Summary Report.

Delgado, A. B., Ricci, S., Chatzopoulou, A., Cegan, Dzurenda, P. & Koutoudis, I. (2023). Enhancing Cybersecurity Education in Europe: The REWIRE's Course Selection Methodology. *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security, 66*(1), 1-7.

Deloitte. (2024). Global Cyber Threat Intelligence (CTI) Annual Cyberthreat Trends Report 2024.*

Digital Skills and Jobs Platform. (2023). Digital Experts: a deep-dive. Retrieved from https://digital-skills-jobs.europa.eu/en/latest/briefs/digital-experts-deep-dive-0.

ECHO. (2021). D2.6 ECHO Cyberskills Framework.

ENISA. (2022a). European Cybersecurity Skills Framework (ECSF): User manual. Retrieved from https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.

ENISA. (2022b). European Cybersecurity Skills Framework (ECSF). Retrieved from https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.

ENISA. (2022c). European Cybersecurity Skills Framework Role Profiles. Retrieved from https://www.enisa.europa.eu/topics/skills-and-competences/skills-development.

Co-funded by the European Union

ENISA. (2022d). Certifications mapped to the ECSF. Retrieved from https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/certifications-mapped-to-the-ecsf.
ENISA. (2023). Identifying emerging Cyber security Threats and Challenges for 2030. *
ENISA. (2024a). Foresight Cybersecurity Threats for 2030 – Extend report 2024. *
ENISA. (2024b). ENISA threat landscape 2024. *
ENISA. (2025). Crosswalk between ESCO and ECSF. Retrieved from https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/crosswalk-between-esco-and-ecsf.
European Commission. (2022a). *COUNCIL RECOMMENDATION of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022H0627(02).
European Commission. (2022b). Education and training monitor 2022. *Directorate-General for Education, Youth, Sport and Culture.* Retrieved from https://op.europa.eu/en/publication-detail/-/publication/cd653a8f-66f4-11ed-b14f-01aa75ed71a1/language-en.
European Commission. (2024). European e-Competence Framework (e-CF). Retrieved from https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf.
European Commission. (2025a). Defining 'Skill' and 'Competence'. Retrieved from https://joint-research-centre.ec.europa.eu/projects-and-activities/skills-and-competences/defining-skill-and-competence_en.
European Commission. (2025b). National Education Systems. Retrieved from https://eurydice.eacea.ec.europa.eu/eurypedia?.
European Union. (2020). User guide to the SME Definition. Retrieved from https://ec.europa.eu/docsroom/documents/42921.
Eurostat. (2024). Participation rate in education and training by sex. Retrieved from *https://ec.europa.eu/eurostat/databrowser/view/trng_aes_100/default/table?lang=en*.
Gallagher, S., Szalay, A., Brandt, A. & Wisniewski, C. (2024). Sophos Threat Report: Cybercrime on Main Street - Ransomware remains the biggest existential cyber threat to small businesses, but others are growing. Retrieved from https://news.sophos.com/en-us/2024/03/12/2024-sophos-threat-report/. *
Gartner (2025). Top 9 Trends in Cybersecurity for 2025. *
HighCharts. (2022). 10 Guidelines for DataViz Accessibility. Retrieved from https://www.highcharts.com/article/10-guidelines-for-dataviz-accessibility/.
Interaction Design Foundation. (2025). User Centered Design (UCD). Retrieved from https://www.interaction-design.org/literature/topics/user-centered-design?srsltid=AfmBOoq6Qg8BsJf0ZYUT1QrWMkxh7UqnY0FO4ydiTmpb9roAfoMa2QD.
ISACA. (2024). State of Cybersecurity 2024 - Global Update on Workforce Efforts, Resources, and Cyberoperations. *
NCSC NZ. (2024). 2023/2024 Cyber Threat Report. *
NCTV. (2024). Cybersecuritybeeld Nederland 2024. *
NOREA. (2025). Legislative Overview 2025. *
NTT Security Holdings. (2024). Global Threat Intelligence Report 2024. *
Polemi, N. & Kioskli, K. (2023). Enhancing Practical Cybersecurity Skills: The ECSF and the CyberSecPro European Efforts. *Human Factors in Cybersecurity, 91*(1), 93-100.
PTvT/Dialogic. (2024). Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity. Retrieved from https://open.overheid.nl/documenten/c0ac3595-28e3-43df-aa85-7d9e8a426c25/file. *

Co-funded by the European Union

PwC. (2025a). Bridging the gaps to cyber resilience: Findings from the 2025 Global. *
PwC. (2025b) Global Digital Trust Insights.
REWIRE. (2023). R.5.2.1. Annual Cybersecurity Skills Trends Report.
REWIRE. (2024). R5.2.1 Third Annual Cybersecurity Skills Trends Report. *
SPARTA. (2021). D9.4 Pilot of Cyber training & exercise Framework (Ct&eF).
World Economic Forum. (2025). Global Cybersecurity Outlook 2025. *

* = report used for Trend Analysis

Co-funded by
the European Union